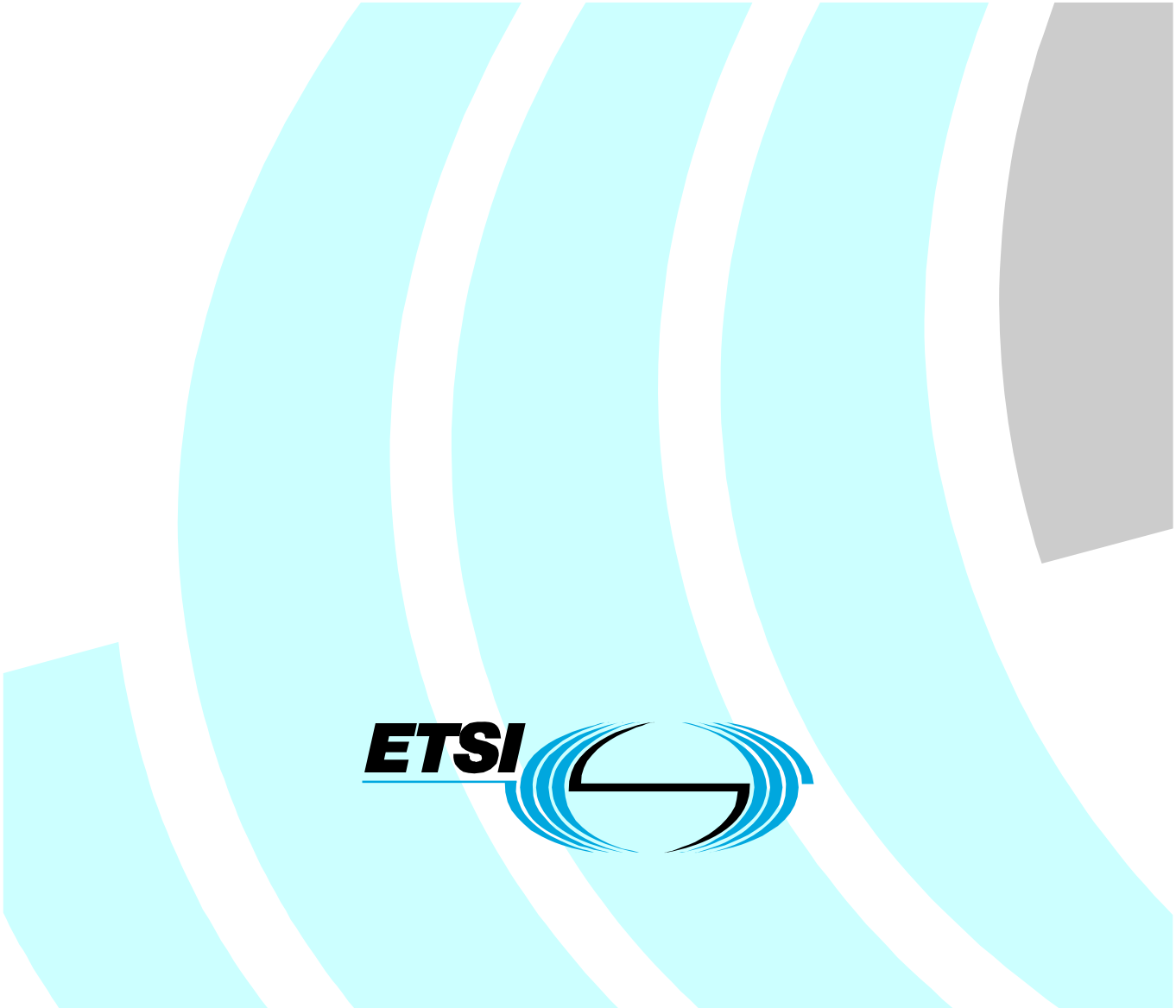
ETSI TS 102 640-1 V1.1.1 (2008-10)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture



Reference
DTS/ESI-000052-1

Keywords
e-commerce, electronic signature, email, security,
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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering Registered Electronic Mail (REM); Architecture, Formats and Policies, as identified below:

Part 1: "Architecture";

Part 2: "Data Requirements and Formats for Signed Evidences for REM";

Part 3: "Information Security Policy Requirements for REM Management Domains".

Introduction

Business and administrative relationships among companies, public administrations and private citizens, are the 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.

Electronic mail is a major tool for electronic business and administration. 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. A range of Registered E-Mail ("REM") services is already established and their number is set to grow significantly over the next few years. Without the definition of common standards there will be no consistency in the services provided, making it difficult for users to compare them. Under these circumstances, users might be prevented from easily changing to alternative providers, damaging free competition. Lack of standardization might also affect interoperability between REM based systems implemented based on different models. The present Technical Specification is to ensure a consistent form of service across Europe, especially with regard to the form of evidence provided, in order to maximize interoperability even between e-mail domains governed by different policy rules.

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 REM, and the ways the electronic signatures are applied to it. In this respect, the electronic signature is an important security component to protect the information and to provide trust in electronic business. It is to be noted that a simple "electronic signature" would be insufficient to provide the required trust to an information exchange. Therefore the present Technical Specification assumes the usage of at least an Advanced Electronic Signature, with the meaning of article 2(2) of EU Directive 1999/93/EC [i.1].

1 Scope

The basic Registered E-Mail service purpose is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of evidences suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service.

The present document specifies an architectural structure of REM. More specifically:

a) describes a logical model for REM including the most relevant REM architectural elements and how they relate to each other (REM-MD Messages, REM Sender, REM Recipient, etc.) and the following styles of operation:

   1) "Store and Forward" (S&F henceforth), were REM Objects are directly forwarded from REM-MDs to the REM Recipient; and

   2) "Store and Notify" (S&N henceforth) were the REM Recipient is first notified of that a REM Object is stored and is provided with a reference to the location where the REM Object can be downloaded;

b) describes how REM components interact using external interfaces to REM users, and interfaces to other REM implementations;

c) describes a policy domain environment; and

d) specifies a list of different types of events and the REM-MD Evidence types that represent them.

Evidential services are deemed to comply with legal, regulatory or contractual requirements to provide legal validity and enforceability under domestic or international law.

The present document does not provide specification for interactions among architectural elements internal to the REM-MD. Although interfaces to physical mail could exist, the present document does not provide standardized interfaces to physical mail.

The structure of the present document is as follows:

- clause 2 contains the list of normative and informative references;
- clause 3 includes definitions of the relevant concepts to the present document and abbreviations;
- clause 4 contains the logical model for REM provision;
- clause 5 specifies REM interfaces; and
- clause 6 provides a list of different types of events and REM-Evidence.

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 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 2: Data Requirements and Formats for Signed Evidences for REM".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

[i.2] IETF RFC 822 (1982): "Standard for the format of ARPA Internet text messages".

[i.3] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.4] IETF RFC 3161 (2001):"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.5] IETF RFC 1305 (1992): "Network Time Protocol (Version 3) Specification, Implementation and Analysis".

3 Definitions and abbreviations

3.1 Definitions

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

Certification Authority: authority trusted by one or more users to create and assign public-key certificates

Information Security Policy: statement of policy which provides management direction and support for information security in accordance with business requirements and relevant laws and regulations

Long Term Storage: role that supports the integrity of data and the authenticity of a signature over the period required to store data for evidential purposes that can be used by the Message Archive

Message archive: optional role that supports storage of REM Objects and REM-MD Evidences, as required for later use for evidential or any other legally admitted purposes, at the relevant REM-MD for an indefinite or definite time period, to be accessed once or many times by one or more entities

Original Message: e-mail message generated by the Sender's User Agent or under the Sender's technical/legal responsibility (i.e. outside of the REM-MD), which may be signed by the Sender

NOTE: It has to be conveyed to the REM Recipient either by value (in the Store & Forward Style of operations) or by reference (in the Store & Notify Style of operations).

REM-MD Repository: role that supports the storage of Original Message, REM-MD Evidence and any other, which must be accessed by reference

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

REM Dispatch: REM-MD Envelope containing the Original Message and related REM-MD Evidence

REM Management Domain (REM-MD): set of technical and physical components, personnel, policies and processes that provide REM services

NOTE: A REM-MD is operated under the responsibility of a single management entity.

REM-MD Envelope: signed structure generated by the REM MD which envelopes an Original message and/or REM-MD Evidence

REM-MD Evidence: signed data created within a REM-MD, which proves that a certain event has occurred at a certain time

NOTE: It may be signed directly or indirectly by placing it within a REM-MD Envelope.

REM-MD Evidence Provider: role that issues REM-MD Evidences

REM-MD Evidence Verifier: role that supports the verification of REM-MD Evidences

REM-MD Message: RFC 822 [i.2] message generated by the REM MD under the REM MD sole technical/legal responsibility (i.e. inside of the REM MD)

NOTE: It must be signed by the entity legally responsible for the REM MD. It may be understood by the REM Recipient/REM Sender as a "receipt" or a "notification". A REM-MD Message carries an REM-MD Envelope containing REM-MD Evidence.

REM-MD Message Gateway: role that supports the transfer of REM objects to conventional e-mail (e.g. Internet) services and physical postal delivery services

REM-MD Message Transfer Agent: role that supports the transfer of REM Objects to REM Recipient's and REM Sender's REM Message Store either directly or via the **REM Object Relay Interface** into another REM-MD or via a REM-MD Message Gateway

REM-MD Repository: role that supports the storage of REM Objects, REM-MD Evidences and any other, which must be accessed by reference

REM-MD Repository Retrieval Interface: interface of REM-MD towards REM UA used in the Store and Notify Style of Operation by the REM Recipient for downloading REM Objects from REM-MD Repository

NOTE: It can also be used by REM Senders for downloading REM-MD Evidences.

REM-MD Sender Message Submission Interface: interface of REM-MD towards sender REM UA used by the REM Sender to submit Original Messages to his REM-MD, for them to be forwarded to the REM Recipients

REM-MD Sender/Recipient Message Store Retrieval Interface: interface of REM-MD towards REM UA used by REM Senders or REM Recipients to fetch REM Objects addressed to them

REM-MD Third Party Evidence Retrieval Interface: interface that supports REM-MD Evidences and REM Objects retrieval by users that are parties external to the usual message flow

REM Message Store: role that supports the storage of REM Objects. In other words the set of mailboxes of the users

REM Object: message object handled by a REM-MD. This is a REM-MD Message, REM-Dispatch or Original message

REM Objects Relay Interface: interface that supports REM objects relaying between disparate REM-MD

REM User Agent (REM-UA): entity by which REM Senders, REM Recipients participate in the exchange of REM Objects and Third Parties may access REM Objects

REM Policy: set of rules (e.g. legal, company policy or agreement) enforced for the provision of REM Services

REM Policy Domain: any domain where a common set of rules (e.g. legal, company policy or agreement) is enforced for the provision of REM services

NOTE: This domain may be a country, a Company, a group of Countries, etc., even a single REM-MD.

REM Policy Domain Authority: authority entitled to enforce the common set of rules in which the REM policy Domain consists

REM Recipient: physical or legal entity legally responsible for the mailbox to which the original message is addressed

REM Sender: physical or legal entity legally responsible for the mailbox from which the original message has been sent

REM Third Party: party authorized to access REM Objects and REM-MD Evidence for specific purposes

Signature Creation Server: server that supports the creation of digital signature against data (e.g. evidence)

Time-Stamping Authority: authority which issues time-stamp tokens (TS 102 023 [i.3])

Time-Stamp Token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time (TS 102 023 [i.3])

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
CAdES	CMS Advanced Electronic Signatures
CEN	Comité Européen de Normalization

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

CMS	Cryptographic Message Syntax
MD-RI	Message and Evidence Relay Interface
RSRI	REM-MD Repository Retrieval Interface
S-MSI	REM-MD Sender Message Submission Interface
S/R-MSRI	REM-MD Sender/Recipient Message Store Retrieval Interface
TP-ERI	REM-MD Third Party Evidence Retrieval Interface
REM	Registered E-Mail
REM-MD	REM Management Domain
REM-PD	REM Policy Domain
REM-UA	REM User Agent
S&F	Store and Forward
S&N	Store and Notify
TSA	Time Stamping Authority
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.

XAdES	XML Advanced Electronic Signature

4 REM Logical Model

This clause specifies a logical model for REM. The model is aimed at supporting a range of REM implementations that may employ different styles of operation.

The model identifies those aspects of the REM that affect external interfaces to REM users, and interfaces to other REM implementations that may employ different styles of operation. Hence, the model is at a high level of abstraction and concentrates on those aspects of REM systems affecting external interfaces. The logical model is not related to any particular implementation.

4.1 REM Functional Viewpoint

The basic elements of the REM Logical Model from the functional viewpoint are illustrated in figure 1.

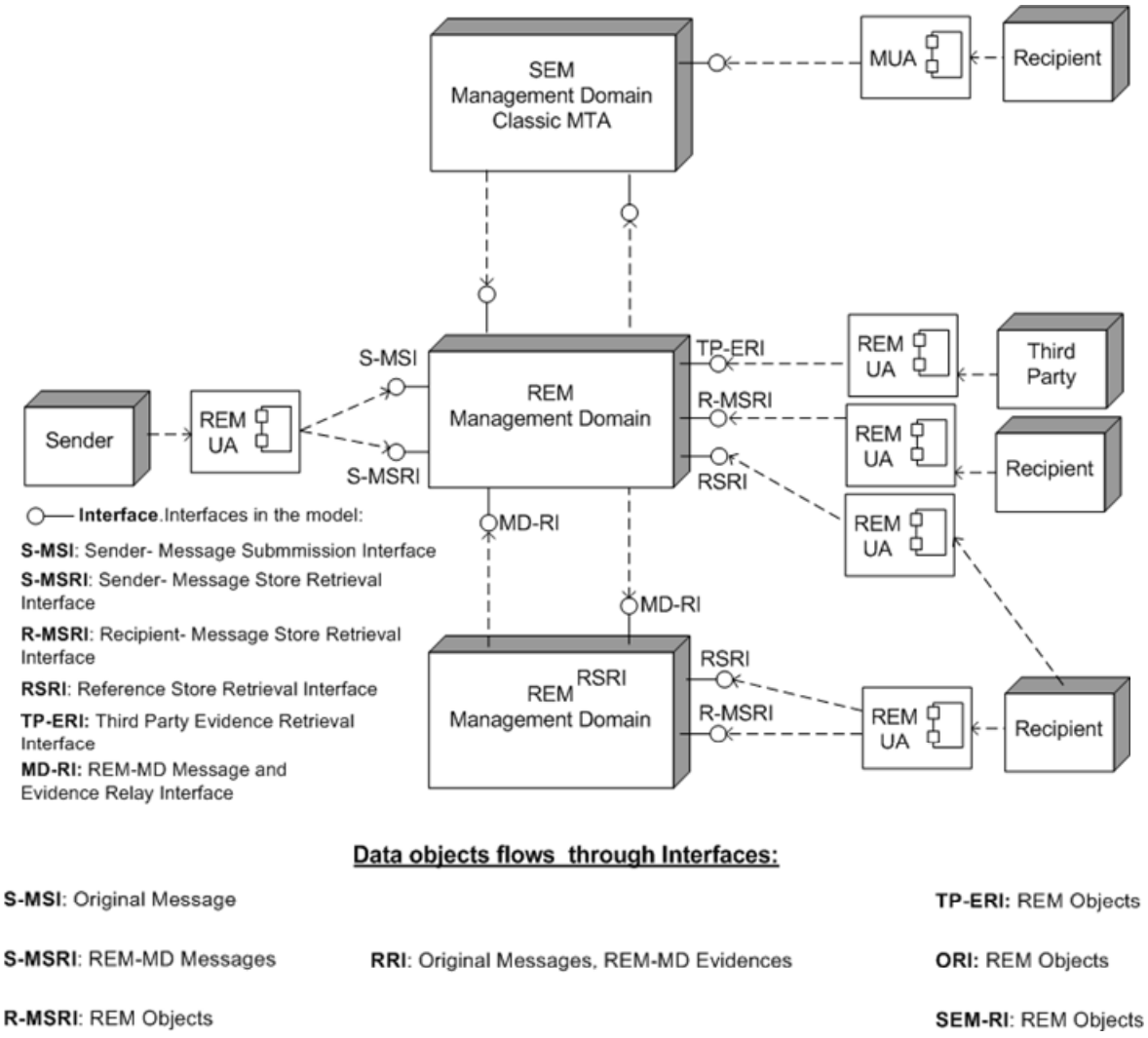


Figure 1: REM Logical Model - Functional Viewpoint

NOTE 1: Arrows indicate service user and provider relationship, their points do not necessarily represent the direction of the exchanged data flow. Circles indicate interfaces for exposing services. Dashed arrows describe use of services through the mentioned interfaces. They do not indicate information flows or direction.

NOTE 2: REM-MD RSRI interface is a mean that can be used also by not-subscriber REM Recipients.

In addition to transport services as provided by existing mailing systems, REM systems provide evidence services related to the submission, transmission (where applicable) and delivery of the REM Object. In particular, evidence services including some or all of evidence types mentioned in clause 6 should be provided to users (be they humans or systems).

The REM users are the REM Sender, the REM Recipient and any Third Party that could be, for instance, the user's organization, a judge in case of dispute, or a party nominated by the REM Sender or REM Recipient for receiving evidences on their behalf. The same entity may act as both REM Sender and REM Recipient.

In most implementations, the REM Sender must authenticate to the relevant REM-Management Domains (REM-MDs), but the choice of the authentication mechanism is left to the specific REM-MD. The REM Sender has access to the REM-MD services through a User Agent.

In some implementations, delivery is subordinated to REM Recipient's explicit acceptance of the new REM Object. To receive REM Objects addressed to him the REM Recipient must authenticate to the relevant REM-MD, but the choice of the authentication mechanism is left to the specific REM-MD.

REM implementation components are broken into REM User Agents (REM-UA) and REM-MDs. The present document envisages those scenarios where two REM-MDs might interoperate together via standard interfaces to provide the REM Object exchange. This is generally the case when the REM Sender and the REM Recipient are not in the same domain and therefore use different REM-MD. In this situation, the REM Object will have to be relayed between disparate REM-MDs.

REM-UA will be used by the REM Sender to send new REM Objects that will be forwarded with Evidence created by one relevant REM-MD, where applicable, as well as for retrieving Evidence generated by any REM-MD. The REM-UA interface to the REM-MD may be realized by two interfaces: one for sending REM Objects the other for receiving REM Objects. A REM UA may interface to more than one REM-MD. The form a User Agent can take is not further specified here. It could be an application installed on user's machine or, in some case, it could be provided as a service by the REM-MD itself (e.g. web mail).

These components interact using the interfaces described in clause 5, namely, REM-MD Sender Message Submission Interface, REM-MD Sender/Recipient Message Store Retrieval Interfaces, REM-MD Repository Retrieval Interface, **REM Object Relay Interface**, Non REM Relay Interface, REM-MD Third Party Evidence Retrieval Interface and REM-MD Repository Retrieval Interface.

4.2 REM Styles of Operation

Two types of REM styles of operation are described below: "Store and Forward" (S&F), and "Store and Notify" (S&N). They can interoperate in a different range of combinations, such as:

a) S&F to S&F, as described in clause 4.2.1;

b) S&N to S&F, where a reference to REM Object contained in a REM-MD Repository is relayed to the REM Recipient's REM-MD using a canonical S&F service;

c) S&N to S&N: in this operational scenario any reference to REM Object contained in a REM-MD Repository sent to a S&N REM-MD is relayed using a S&F service and it is handled, at REM Recipient's REM-MD's side by a S&F sub-component;

d) S&F to S&N, as described in figure 4.

4.2.1 REM Store and Forward Style of Operation

This clause describes the style of operation "Store and Forward" (S&F henceforth). Under this style of operation REM Objects are directly forwarded from REM-MDs to the REM Recipient, certain REM-MD Messages are directly forwarded from REM-MDs to the REM Sender of the Original Message, and certain REM-MD-Messages (see clause 6) are directly forwarded from REM-MDs to the REM Recipient of the Original Message.

Figure 2 shows two REM-MDs working under S&F style of operation interacting. A subscriber of the first REM-MD sends (this subscriber acts as REM Sender) a REM Object to a subscriber of the second REM-MD (this subscriber acts as REM Recipient of the Original Message). The figure shows an example of how the different REM Objects would flow among the different actors (REM-MDs and subscribers).

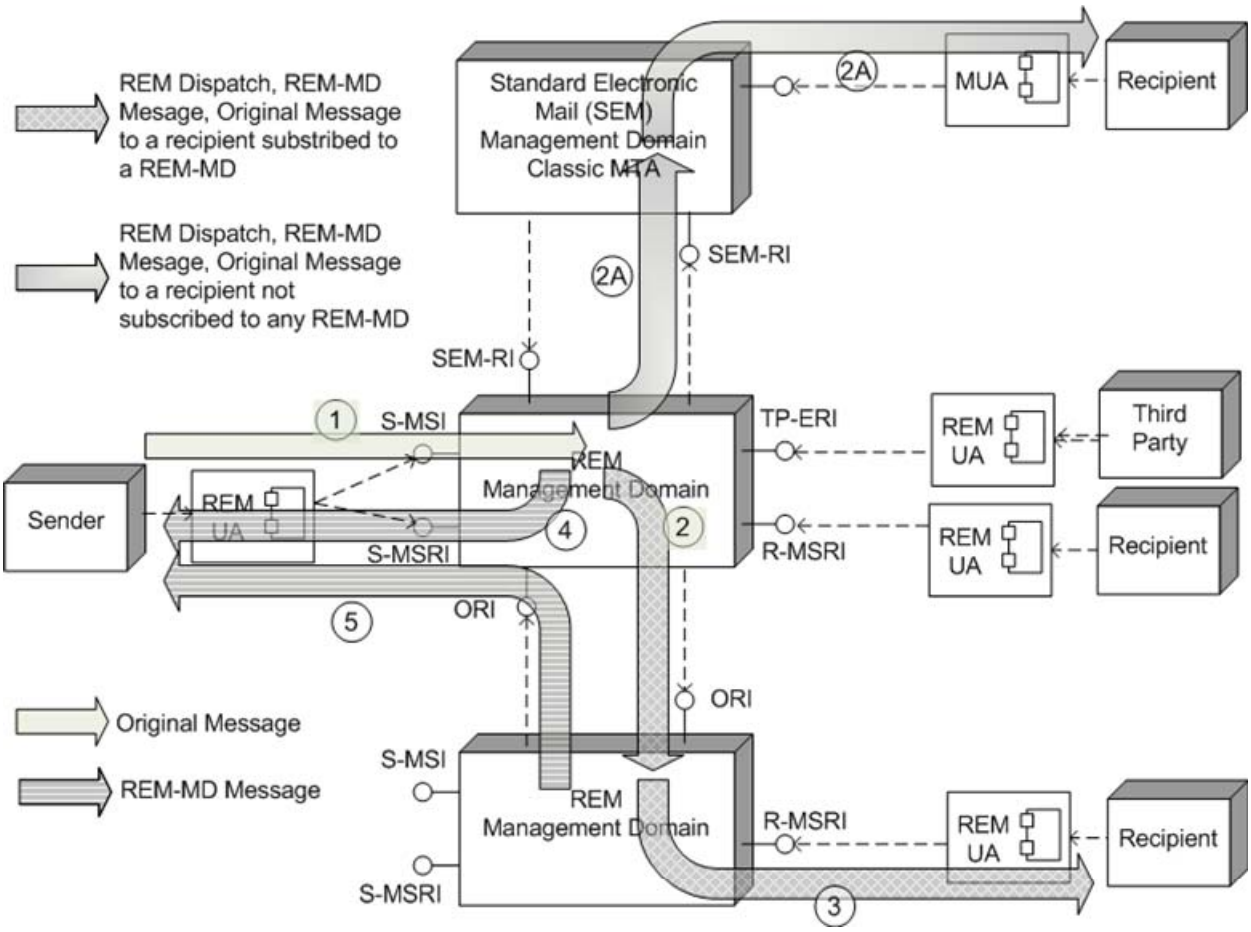


Figure 2: REM Store & Forward Logical Model - REM Sender and REM Recipient subscribers of different REM-MDs

In figure 2:

a) the REM Sender submits, through the REM-MD Sender Message Submission Interface, the Original Message addressed to the **REM Recipient** (flow 1 in figure 2);

b) the REM Sender's REM-MD may generate REM-MD Evidences for the REM Recipient. It may then create and forward a REM Dispatch including the Original Message and the aforementioned REM-MD Evidences, to the Recipient's REM-MD, Alternatively it may create a REM-MD Message containing only the REM-MD Evidences and separately forward this REM-MD Message and the Original Message to the Recipient's REM-MD through the **REM Object Relay Interface** (flow 2 in figure 2). Should the Recipient not be subscribed to any REM-MD, the Sender's REM-MD would forward the REM Object to the standard e-mail management domain through the Non-REM Relay Interface (SEM-RI in figure 2) (flow 2A in figure 2);

NOTE: Where a REM-MD Message is forwarded by one REM-MD to a non REM-MD it MAY contain no REM-MD Evidence.

c) the **REM Recipient**'s REM-MD receives any of the REM Objects aforementioned. It may generate new REM-MD Evidences. It may then deliver a REM Dispatch with the Original Message and any REM-MD Evidence generated so far, or separately forward the Original Message and REM-MD Messages with REM-MD Evidences, to the REM Recipient through the Recipient Message Store Retrieval Interface (flow 3 in figure 2);

d) in addition to the former actions and flows, a REM Sender's REM-MD may also generate specific REM-MD Evidences addressed to the REM Sender and deliver a REM-MD Message containing these REM-MD Evidences, through the REM-MD Sender Message Store Retrieval Interface (flow 4 in figure 2).

e) upon delivery in the REM Recipient's mailbox, or in case of non-delivery, the REM Recipient's REM-MD generates the corresponding REM-MD Evidence and sends a REM-MD Message containing such REM-MD Evidence addressed to the REM Sender. This REM-MD Evidence informs the REM Sender that the Original Message has been delivered/non delivered to the REM Recipient's mailbox (flow 5 in figure 2).

The present clause does not provide details on the sequence of events leading to the generation of REM-Evidences, nor establishes rules on when, how or by whom these REM-Evidence will be incorporated into a REM Object A sequence is detailed in annex A, although a different set of actions and flows may also be present in actual implementations.

REM-Evidences and formats for REM Objects flowing from one REM-MD to another using different technology are fully specified in TS 102 640-2 [1].

4.2.2 REM Store and Notify Style of Operation

This clause describes the style of operation "Store and Notify" (S&N henceforth). Under this style of operation an Original Message or a REM-MD Evidence is not directly forwarded to the REM Recipient.

The REM Sender's REM-MD stores the Original Message in its REM-MD Repository and creates a REM-MD Message for the REM Recipient that includes reference to REM-MD Repository. This reference to REM-MD Repository is made of a generic text, informing the REM Recipient that a REM Object intended for him/her is stored in the REM Sender's REM-MD's storage, and of a reference to the location where such REM Object can be downloaded from.

In this model, a REM-MD provides additional interfaces for REM Senders and/or REM Recipients to access Original Message and/or REM-MD Evidence

The use of Store and Notify for the case where the REM Sender REM-MD supports store and notify is shown in figure 3.

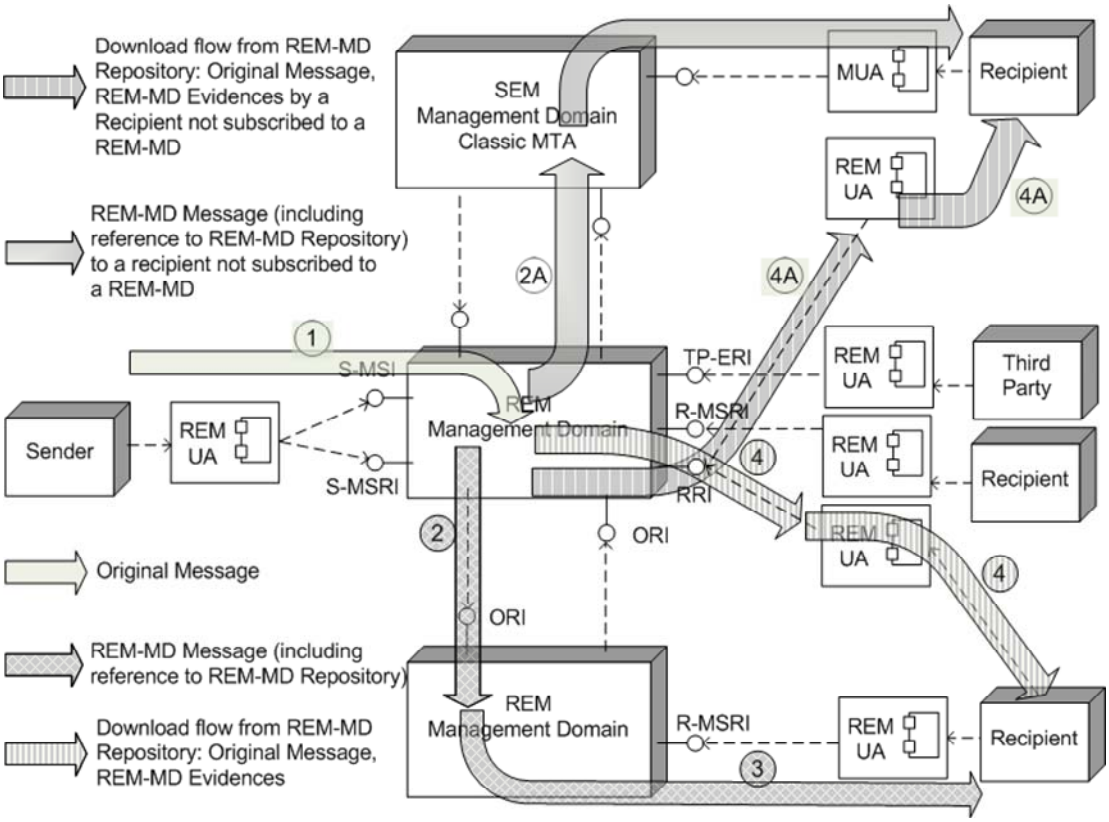


Figure 3: REM Store & Notify Logical Model - REM Sender's REM-MD creating the REM-MD Message

The flow and process steps as illustrated in figure 3 for this case are as follows:

a) the **REM Sender** submits the Original Message, addressed to the REM Recipient, through the REM-MD Sender Message Submission Interface (flow 1 in figure 3);

b) the REM Sender's REM-MD:

1) stores the REM Object in the REM-MD Repository;

2) creates a REM-MD Message that contains a reference to the REM Object within the REM-MD Repository;

3) adds any appropriate REM-MD Evidence to the aforementioned REM-MD Message or stores the REM-MD Evidence in the REM-MD Repository; and

4) forwards this REM-MD Message to the REM Recipient's REM-MD using the **REM Object Relay Interface** (flow 2 in figure 3). Should the Recipient not be subscribed to any REM-MD, the Sender's REM-MD would forward the REM-MD Message to the standard e-mail management domain through the Non-REM Relay Interface (SEM-RI in figure 3) (flow 2A in figure 3);

NOTE 1: This REM-MD Message could be forwarded to the REM Recipient via an ordinary e-mail provider, but in this case its delivery would be out of the REM control.

c) the REM Recipient's REM-MD forwards the REM-MD Message to the REM Recipient using the REM-MD Recipient Message Store Retrieval Interface (flow 3 in figure 3);

d) the REM Recipient downloads the REM Object (and the REM-MD Evidences if they are stored in the REM-MD Repository) from the REM Sender's REM-MD Repository through the REM-MD Repository Retrieval Interface. (flow 4 in figure 3). Should the Recipient be not subscribed to any REM-MD, still she would download the corresponding REM Object from the REM Sender's REM-MD Repository through the aforementioned interface (flow 4A in figure 3).

The use of store and notify for the case where the REM Recipients domain supports store and notify is shown in figure 4.

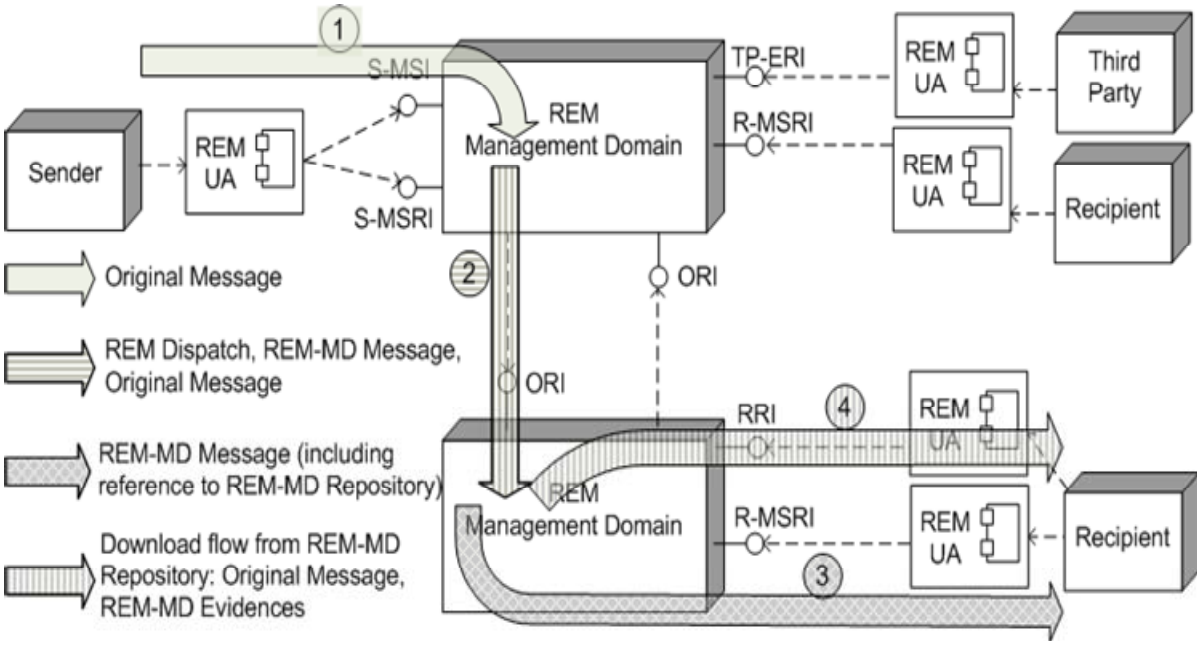


Figure 4: REM Store & Notify Logical Model - Recipient's REM-MD creating the REM-MD Message

In figure 4:

a) the REM Sender submits the Original Message addressed to the **REM Recipient** through the REM-MD Sender Message Submission Interface (flow 1 in figure 4);

b) the REM Sender's REM-MD forwards the REM Object to the **REM Recipient**'s REM-MD through the **REM Object Relay Interface** (flow 2 in figure 4);

c) the **REM Recipient**'s REM-MD:

1) stores the REM Object;

2) creates a REM-MD Message that contains a reference to the REM Object within the REM-MD Repository;

3) adds any appropriate REM-MD Evidence to the aforementioned REM-MD Message or stores the REM-MD Evidence in the REM-MD Repository; and

4) delivers this REM-MD Message to the **REM Recipient**, through REM-MD Recipient Message Store Retrieval Interface (flow 3 in figure 4).

d) the **REM Recipient** downloads the REM Object (and the REM-MD Evidences if they are stored in the REM-MD Repository) from the **REM Recipient**'s REM-MD storage through the REM-MD Repository Retrieval Interface (flow 4 in figure 4).

NOTE 2: Depending on the implementation the **REM Recipient** may be also asked to accept/reject downloading the REM Object or the REM Evidence stored in the REM-MD repository.

Hybrid implementations of this model may pass only some REM Object and/or REM-MD Evidence by reference, the rest being carried "in-band". For example: the data text can be carried in a REM-MD Message while attachments are referenced via a URL.

The data flow to the user is separated from the flow informing the **REM Recipient** of the presence of that data as illustrated above.

Signatures will be applied as specified in TS 102 640-2 [1].

4.3 Roles within a REM MD

As illustrated in figure 5, the logical model refines the REM-MD into separate roles. A role represents some externally visible aspect of the functionality provided within a REM-MD or related to it. An implementation component may carry out one or more roles in supporting REM Services, as described in this clause. In addition, the same role may be supported by several implementation components.

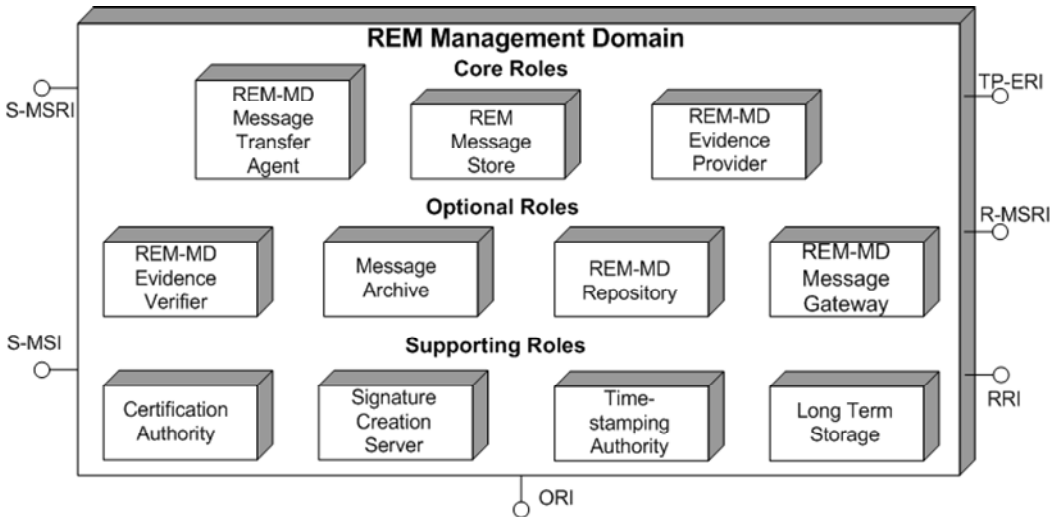


Figure 5: Roles within a REM-MD

The REM-MD shall include the following Core Roles: REM-MD Message Transfer Agent, REM Message Store, and REM-MD Evidence Provider. A REM Message Store is allocated to the REM Senders and **REM Recipient**s and is securely accessible by REM Sender and **REM Recipient**s respectively to retrieve REM Objects addressed to them.

The REM-MD may also include components supporting the following optional roles as described in figure 5: Message Archive, REM-MD Repository, REM-MD Evidence Verifier, and REM-MD Message Gateway.

A REM-MD Message Gateway supports the transfer of REM-MD Messages to and from external conventional e-mail (e.g. Internet) services to physical postal delivery services, as follows:

a) **Gateway to physical mail:** Where Original Messages are required by the REM Sender to be printed and forwarded by surface mail, or where this option is explicitly covered in the agreements between one REM-MD and its users. Please refer to clause 6 for further details on REM-MD Evidence. No general protocol is specified.

NOTE: Transfer of physical mail to a **REM Recipient** is outside the scope of the present document, since, when enacted, it is a mechanism purely internal to the specific REM-MD that can, therefore, implement it autonomously.

b) **Gateway to ordinary e-mail:** users of a REM-MD should be able to exchange REM Objects in electronic form with non REM users. In fact, in some specific cases, the REM-MD user's needs might be satisfied by the possibility to exhibit the trusted REM-MD Evidence of just having sent to a certain Recipient a specific REM Object at a certain time (i.e. the REM-MD Evidence of acceptance of the sent REM Object by the relevant REM-MD). Similarly, their needs might be satisfied by being able to exhibit trusted REM-MD Evidence that a certain REM Object, someone sent them, was actually received through their REM-MD at a certain time. Please refer to clause 6 for further details on REM-MD Evidence. Clause 5 of TS 102 640-2 [1] covers in detail these topics.

The following supporting roles may be used by the ones listed above in support of their functions as described in figure 5: Certification Authority (CA), Signature Creation Server, Time-Stamping Authority (TSA) and Long Term Storage.

Were entities and REM users are not equipped, or willing, to issue themselves signatures (e.g. on the REM-MD Evidence or the forwarded Original Message), they can take advantage of external Signature Creation Servers. The specific entity shall forward the to-be-signed object to the Signature Creation Server. Being this service provision most likely governed by a bilateral contractual relationship, the format and timing of the REM-MD Evidence is left up to these contracts, therefore no general protocol is specified.

Time Stamping Authority is an independent entity that issues Time Stamping Tokens of the submitted digests (protocols specified in RFC 3161 [i.4] may apply). Concerning reliable time provider, trusted time providers can be used by any entity issuing the above mentioned REM-MD Evidences (the NTP - RFC 1305 [i.5] - specifications may be used).

Among these supporting roles the CA and TSA roles MUST NOT be in sourced. These services are intended to provide an additional layer of trust that only an entity third is able to give.

4.4 REM Administrative Viewpoint

From a policy and administrative viewpoint a set of REM-MDs may be grouped in Policy Domains as described in figure 6.

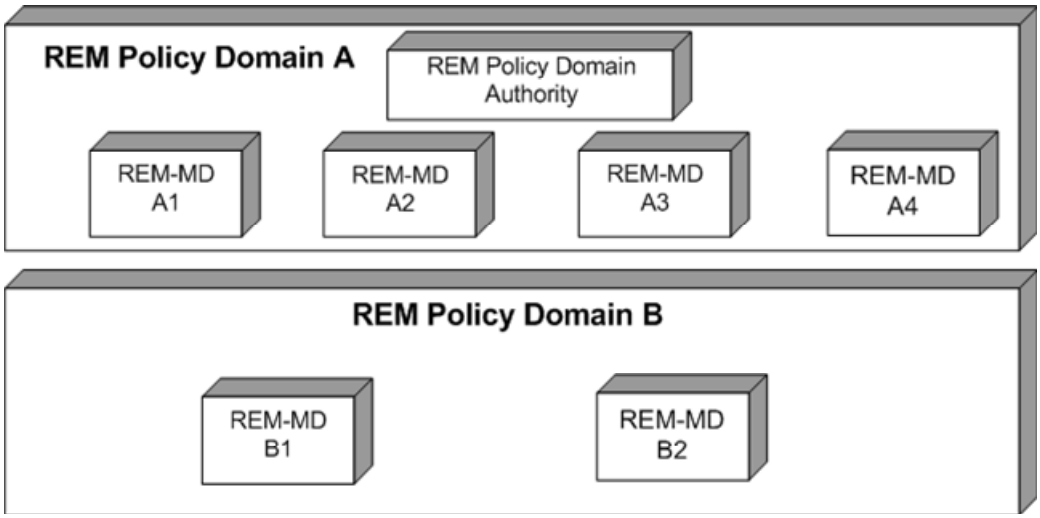


Figure 6: Logical grouping of REM-MDs in a policy domain

A REM Policy Domain may have an Authority supervising the application of the policy and, within one REM-PD, there may be one or more REM-MD that provide end users with the whole set of REM related services.

A REM-MD may belong to more than one REM-PD, provided that it complies with the rules of all of them. For example, a REM-MD set up in one country by a multinational company could be compliant to the sets of rules of both the relevant country and the multinational company.

5 REM Interfaces

REM components, as described in clause 4.1, interact using the following interfaces:

REM-MD Sender Message Submission Interface: this interface is used by the user acting as a REM Sender to submit REM Objects to his REM-MD, for them to be forwarded to the REM Recipients. It is recommended that REM Objects are submitted using SMTP protected using TLS/SSL. The user may authenticate using passwords if protected and only used with an authenticated server. (e.g. using TLS/SSL).

NOTE 1: Other protocols apart SMTP are allowed for REM-MD Sender Message Submission Interface.

REM-MD Sender/Recipient Message Store Retrieval Interfaces: this interface is used by REM Senders or **REM Recipient**s to fetch REM Objects trough a reference to REM-MD Repository addressed to them. It is recommended that REM Objects are retrieved using pop3 or imap protected using TLS/SSL. The user may authenticate using passwords if protected and only used with an authenticated server. (e.g. using TLS/SSL).

REM-MD Repository Retrieval Interface: this interface is used in the Store and Notify Style of Operation by the **REM Recipient** for downloading REM Objects or REM-MD Evidences from a REM-MD Repository. It can also be used by REM Senders for downloading REM-MD Evidence.

It is recommended that REM Objects or REM-MD Evidences are retrieved using HTTP or FTP as identified using a URL protected using TLS/SSL. The user may authenticate using passwords if protected and only used with an authenticated server. (e.g. using TLS/SSL).

REM Object Relay Interface: the Relay interface allows REM Object and related REM-MD Evidences to be relayed between disparate REM-MDs. It is recommended that REM Object are relayed between REM-MDs using S/MIME over SMTP.

Non REM Relay Interface: this interface is provided to allow client-based REM Object retrieval and web-based REM Object retrieval. It is recommended that REM Object are relayed using S/MIME over SMTP.

REM-MD Third Party Evidence Retrieval Interface: this interface is provided to allow REM-MD Evidence and REM Object retrieval by users that are parties external to the usual message flow. These users might require access to REM-MD Evidence in some specific cases (i.e., a tribunal in case of dispute, or a third party nominated by the REM Sender or **REM Recipient** for receiving REM-MD Evidence on their behalf).

NOTE 2: The present document does not standardize this interface.

6 REM Events and REM-MD Evidence

6.1 Overview

In this clause the REM Events represented by REM-MD Evidence types are listed, along with a brief description of what event each REM-MD Evidence has the Purpose to state. Issued REM-MD Evidence can serve more purposes by including information related to more Events. The REM-MD Evidence topic is extensively addressed in TS 102 640-2 [1], clause 5.1 that covers also the REM-MD Evidence general structure and the content of each REM-MD Evidence type, as described in table 1.

Table 1: Event types and content of REM-MD Evidence

Event and REM-MD Evidence	REM-MD Evidence (TS 102 640-2 [1], clause 5.1)
6.2.1 Event A.1 - S-REM-MD Acceptance	5.1.1 SubmissionAcceptanceRejection
6.2.1 Event A.2 - S- REM-MD Rejection	
6.2.2 Event B.1 - R-REM-MD Acceptance	5.1.2 RelayToREMMDAcceptanceRejection
6.2.2 Event B.2 - R-REM-MD Rejection	
6.2.2 Event B.3 - Expiration of time to deliver to R-REM-MD	5.1.3 RelayToREMMDFailure
6.2.3 Event C.1 - REM Object Delivery	5.1.4 DeliveryNonDeliveryToRecipient
6.2.3 Event C.2 - Non delivery within a given retention period	
6.2.3 Event D.1 - REM-MD Message Delivery	
6.2.3 Event D.2 - Expiration of time to deliver	
6.2.3 Event E.1 (REM-MD Repository) Download	5.1.5 DownloadNonDownloadByRecipient
6.2.3 Event E.2 (REM-MD Repository) Expiration of time for download	
6.2.3 Event E.4 (REM-MD Repository) Download by a REM Recipient's delegate	
6.2.3 Event F.1 (mailbox) - Retrieval	5.1.6 RetrievalNonRetrievalByRecipient
6.2.3 Event F.2 (mailbox) - Expiration of time for Retrieval	
6.2.3 Event F.3 (mailbox) - Retrieval by a REM Recipient's delegate	
6.2.3 Event E.3 - Rejection of download by REM Recipient	5.1.7 AcceptanceRejectionByRecipient
6.2.4 Event H.1 - Successful forwarding for Ordinary e-mail	5.1.8 RelayToNonREMSystem
6.2.4 Event H.2 - Unsuccessful forwarding for Ordinary e-mail	
6.2.4 Event G.1 - Successful forwarding for Printing	
6.2.4 Event G.2 - Unsuccessful forwarding for Printing	
6.2.4 Event I.1 - E-mail message received from a regular e-mail system	5.1.9 ReceivedByNonREMSystem

One REM Object can optionally be electronically signed by the REM Sender to provide the REM Recipient with information on the REM Object origin and authenticity. Similarly, each REM-MD Evidence can optionally be signed. At least the REM Object AND/OR all of the REM-MD Evidence it carries SHALL be signed. The REM Recipient can deem this information as reliable if the certificate supporting the signature is issued by a Certification Authority that the REM Recipient acknowledges as trusted (see note) and, where required, if the signature is issued by means of a Secure Signature Creation Device with the meaning of article 2(6) of the Directive 1999/93/EC [i.1]. Other signature attributes cannot be automatically inferred as reliable, for example the signing time that derives from the REM Sender's system that is not per se a trusted entity.

NOTE: As an example, in the European Union, Certification Authorities issuing Qualified Certificates, as defined in the European Directive 1999/93/EC [i.1], article 2(10), are trusted since article 3(3) of the same Directive mandates that they are supervised in the EUMS they reside in.

It is assumed that the signature is at least an Advanced Electronic Signature (AdES) as defined in Directive 1999/93/EC [i.1] of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Depending on the applicable legislation, this AdES can be supported with a QC and/or issued with a SSCD.

6.2 Event Types and their Proof

In this clause the Events related to the basic REM functions are listed, logically grouped on the basis of what the related REM-MD Evidence types have the purpose to prove.

In order to facilitate interoperability and based on the outcomes of a survey performed among a large number of interviewees, the REM-MD Evidence type related to each event below is indicated as "M" (mandatory), "R" (recommended) or "O" (optional).

6.2.1 Events and REM-MD Evidence related to the REM Sender's REM-MD

A. Submission

1) Submission acceptance

Purpose of the related REM-MD Evidence: to prove that a certain REM Object was successfully submitted, at the time indicated in the REM-MD Evidence, to the REM Sender's REM-MD by the REM Sender upon authentication by the REM Sender's REM-MD.

REM-MD Evidence Optionality: "M"

2) Submission non acceptance

Purpose of the related REM-MD Evidence: to prove that a certain REM Object that was submitted, at the time indicated in the REM-MD Evidence, to the REM Sender's REM-MD by the REM Sender upon authentication by the REM-MD, was not accepted by the REM Sender's REM-MD.

REM-MD Evidence Optionality: "M"

6.2.2 Events and REM-MD Evidence related to the REM Recipient's REM-MD

B. Reception by the REM Recipient's REM-MD

1) REM Object acceptance by the REM Recipient's REM-MD

Purpose of the related REM-MD Evidence: to prove that one REM Object sent by the REM Sender's REM-MD and successfully received by the **REM Recipient**'s REM-MD, was accepted by the latter.

REM-MD Evidence Optionality: "R"

2) REM Object rejection by the REM Recipient's REM-MD

Purpose of the related REM-MD Evidence: to prove that one REM Object sent by the REM Sender's REM-MD and successfully received by the **REM Recipient**'s REM-MD, was rejected by the latter due to policy, formal or technical reasons.

REM-MD Evidence Optionality: "O"

3) Non delivery within a given time period of the REM Object to the REM Recipient's REM-MD

Purpose of the related REM-MD Evidence: to prove that it was impossible to deliver within a given time period a REM Object to the **REM Recipient**'s REM-MD due to technical errors and/or other problems.

NOTE: This may depend on:

a) it is impossible for the REM Sender's REM-MD to identify the REM Recipient's REM-MD;

b) the REM Recipient's REM-MD is unreachable;

c) the REM Recipient's REM-MD rejected the REM Object for any reason.

REM-MD Evidence Optionality: "R"

6.2.3 Events and REM-MD Evidence related to the REM Recipient

C. REM Object delivery

1) Delivery

Purpose of the related REM-MD Evidence: to prove that the REM Object was delivered to the REM Recipient's mailbox at a specific time.

REM-MD Evidence Optionality: "M"

2) Non delivery within a given retention period

Purpose of the related REM-MD Evidence: this REM-MD Evidence type has two purposes:

1) to prove that the REM Object could not be delivered to the REM Recipient's mailbox within a given time period due to technical errors and/or other reasons;

2) to indicate that no prove of delivery within a given period exists.

The time limit is fixed by statutory or contractual rules, or it is pre-defined by the REM Sender.

NOTE 1: The REM-MD Evidence applies to the following two different events:

i) the REM Recipient's REM-MD sends back to the REM Sender's REM-MD the REM-MD Evidence of delivery/non delivery, to be forwarded to the REM Sender, in this case this REM-MD Evidence is generated by the REM Recipient's REM-MD;

ii) the REM Sender's REM-MD, after having received from the REM Recipient's REM-MD the REM-MD Evidence that it accepted the REM Object to be delivered to the REM Recipient's mailbox, does not receive within a given time period from the same REM-MD the REM-MD Evidence as in item C.1; in this case the REM Sender's REM-MD will create this REM-MD Evidence with a suitable reason code to indicate the event type.

REM-MD Evidence Optionality: "M"

D. REM-MD Message delivery

1) Delivery to the REM Recipient's mailbox of a reference to REM-MD Repository **that a REM Object is available for downloading**

Purpose of the related REM-MD Evidence: to prove that the **REM Recipient**'s REM-MD delivered to the **REM Recipient**'s mailbox a reference to REM-MD Repository **that a REM Object** is ready to be downloaded from a REM-MD Repository.

REM-MD Evidence Optionality: "M"

2) Non delivery to the REM Recipient's mailbox within a given period of a REM-MD Message that a REM Object is stored and available to be downloaded

Purpose of the related REM-MD Evidence: this REM-MD Evidence type has two purposes:

1) to prove that the REM MD Message could not be delivered to the **REM Recipient**'s mailbox within a given time period due to technical errors and/or other reasons;

2) to indicate that no prove of delivery within a given period exists.

The time limit is fixed by statutory or contractual rules, or it is pre-defined by the REM Sender.

NOTE 2: The REM-MD Evidence applies to the following two different events:

i) the REM Recipient's REM-MD sends back to the REM Sender's REM-MD the REM-MD Evidence of delivery/non delivery, to be forwarded to the REM Sender, in this case this REM-MD Evidence is generated by the REM Recipient's REM-MD;

ii) the REM Sender's REM-MD, after having received from the REM Recipient's REM-MD the REM-MD Evidence that it accepted the REM-MD Message to be delivered, does not receive within a given time period from the same REM-MD the REM-MD Evidence as in item D.1.; in this case the REM Sender's REM-MD will create this REM-MD Evidence with a suitable reason code to indicate the event type.

REM-MD Evidence Optionality: "M"

E. REM Object download

1) Download

Purpose of the related REM-MD Evidence: to prove that the REM Object was downloaded by the REM Recipient or by a delegate at a specific time.

REM-MD Evidence Optionality: "M"

2) Non download within a given retention period (see also item 14)

Purpose of the related REM-MD Evidence: to prove that the REM Object was not downloaded within a given period from the REM-MD Repository under the responsibility of the REM Recipient's REM-MD due to technical errors and/or other reasons.

The time limit is fixed by statutory or contractual rules, or it is pre-defined by the REM Sender.

REM-MD Evidence Optionality: "M"

3) Rejection by the REM Recipient of the REM Object to be downloaded

Purpose of the related REM-MD Evidence: to prove that the REM Object to be downloaded was rejected by the **REM Recipient**.

REM-MD Evidence Optionality: "R"

4) Download by an entity delegated by the REM Recipient

Purpose of the related REM-MD Evidence: to prove that the REM Object was downloaded by some entity delegated by the **REM Recipient**.

REM-MD Evidence Optionality: "O"

F. Content retrieval

1) Retrieval

Purpose of the related REM-MD Evidence: to prove that the REM Object present in the **REM Recipient**'s mailbox was retrieved by the **REM Recipient**.

NOTE 3: This **REM-MD Evidence** type is referred to the moment the **REM Recipient** actually accesses its mailbox with a mail client, be it an asynchronous client (like Outlook, Thunderbird, etc.) or a webmail client.

REM-MD Evidence Optionality: "O"

2) Non retrieval within a given period

Purpose of the related REM-MD Evidence: to prove that the REM Object present in the **REM Recipient**'s mailbox was not retrieved by the **REM Recipient**'s mail client within a given period.

REM-MD Evidence Optionality: "O"

3) REM Object retrieval by an entity delegated by the REM Recipient

Purpose of the related REM-MD Evidence: to prove that the REM Object was retrieved by some entity delegated by the **REM Recipient**.

REM-MD Evidence Optionality: "O"

6.2.4 Events and REM-MD Evidence related to connections with outside the REM-MD

G. Printing

1) The Original Message was successfully submitted to a printing system to be subsequently sent via physical registered mail

Purpose of the related REM-MD Evidence: to prove that a certain Original Message was, on behalf of the REM Sender's or REM Recipient's REM-MD, successfully printed to be forwarded via physical registered mail.

NOTE 1: The Original Message can also be printed to be forwarded through physical registered mail on behalf of the REM Sender's or REM Recipient's REM-MD, in case the Original Message cannot be delivered into the REM Recipient's mailbox only if a specific statutory or contractual requirement exists to enact such forwarding.

REM-MD Evidence Optionality: "O"

2) The submission to a printing system of the Original Message to be subsequently sent via physical registered mail was unsuccessful

Purpose of the related REM-MD Evidence: to prove that the REM Sender's or REM Recipient's REM-MD was unable to submit the Original Message to a printing system to subsequently forward it to physical registered mail.

NOTE 2: See note in previous **REM-MD Evidence**.

REM-MD Evidence Optionality: "O"

H. Forward to regular e-mail

1) The REM Object was successfully forwarded to a regular e-mail service

Purpose of the related REM-MD Evidence: to prove that a certain REM Object was successfully forwarded on behalf of the REM Sender's or of the REM Recipient's REM-MD to a regular e-mail service.

NOTE 3: Depending on the statutory or contractual agreements, the REM Sender's REM-MD or the REM Recipient's REM-MD can forward a REM Object to ordinary e-mail also if it is not able to forward it to the REM Recipient's REM-MD via REM.

REM-MD Evidence Optionality: "O"

2) The REM Object forwarding to regular e-mail was unsuccessful

Purpose of the related REM-MD Evidence: to prove that the REM Sender's or REM Recipient's REM-MD was not able to forward a REM Object to a regular e-mail service.

REM-MD Evidence Optionality: "O"

I. Non REM origin

1) E-mail message was successfully received from a regular e-mail system

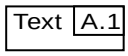
Purpose of the related REM-MD Evidence: to prove that a certain email was not received from a REM-MD but from an ordinary e-mail server, therefore all information related to its sending, like the REM Sender's address and the sending time, cannot be trusted per se.

Annex A (informative): REM Events and Actions flows

Figure A.1 describes the sequence of actions performed by the involved entities (from the REM Sender up to the REM Recipient or to external entities, like regular e-mail server or printer server) and of the related events that lead to issuance and delivery of REM-MD Evidence. Event types are not indicated: they are detailed in clause 6.2.

1) Actions - Every action, to each of which one row is dedicated, is indicated in the column of the entity that performs it. From each action, arrows point to the entities the same action is directed to or to the events described in the related REM-MD Evidence, as specified in clause 6.2. These events are represented with boxes having this appearance: 

.

2) Events - Events are represented with boxes having the following appearance: 

where the text describes the related event, as indicated in clause 6.2, and the small box inside refers to the event type as numbered in the same clause 6.2. Boxes related to successful events have a white background, those referring to unsuccessful ones have a background that prints in gray.

3) Junctions, i.e. where one action can produce more that one event, or one event is followed by more other events that can occur alternatively, are represented with a circle  . Where applicable, black circles with white numbers inside indicate the sequence with which the events occur.

4) The symbol  indicates the entity to which an REM-MD Evidence, consequent to one event, is delivered. Connections to this symbol are in dotted arrows.

One REM-MD Message MAY refer to another REM-MD Message referring in turn to the final Original Message to be downloaded, therefore REM-MD Message Delivery (Action No 5) and REM Object download (Action No 6) can be iterated.

NOTE: Due to space restrictions the terms defined in clause 3.1 are shortened also by removing terms like REM and REM-MD where necessary.

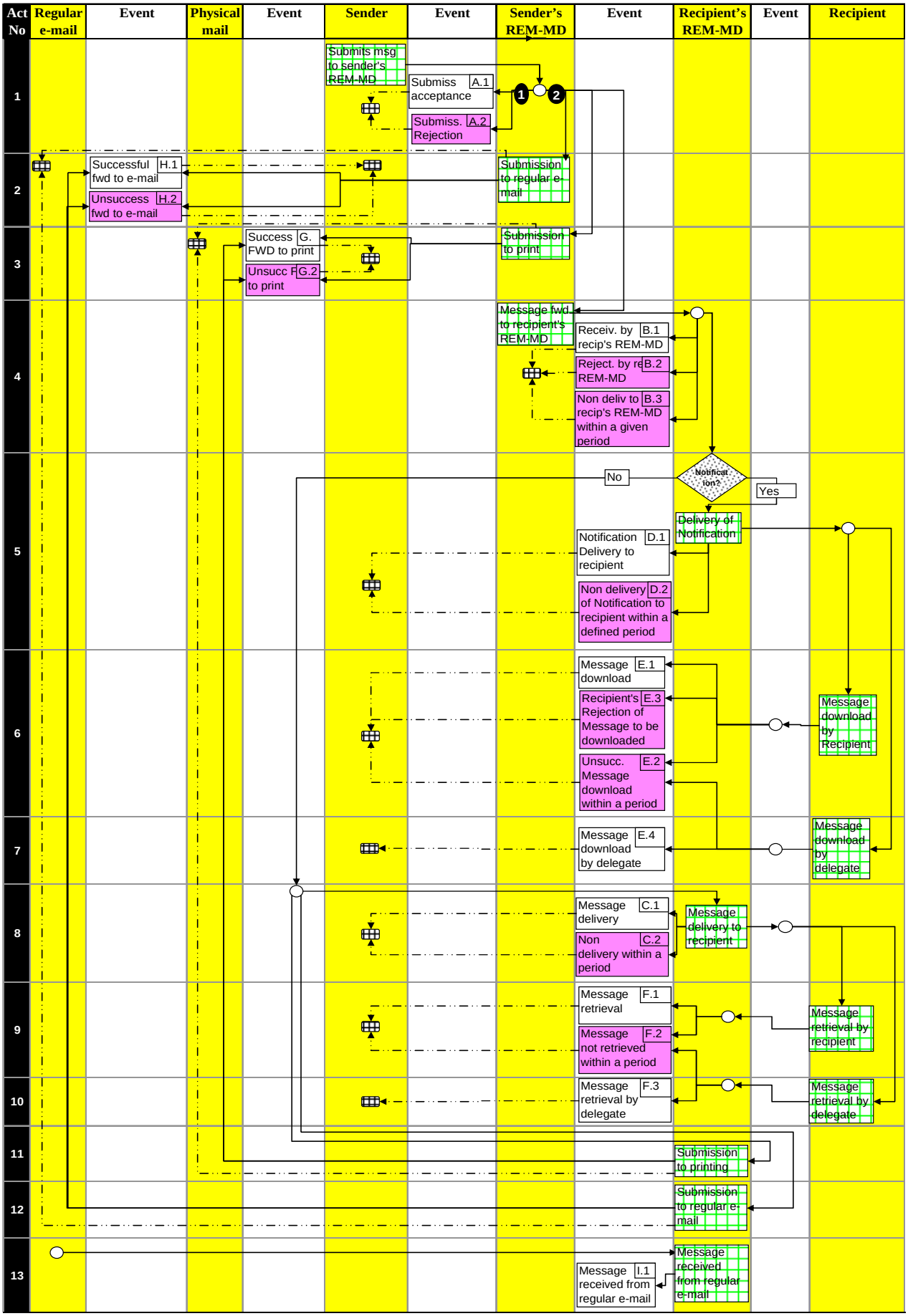


Figure A.1: Actions sequence

Figure A.2 specifies the sequence of the events performed when REM Object flow from one end (namely the REM Sender) to another end that can be the REM Recipient or provider of ordinary e-mail services or of printing services.

1) *Events* - Events are represented with boxes having the following appearance: A.1 Text where the text describes the related event and the small box inside refers to the event number as in the following clauses. Boxes related to successful events have a white background.

   Boxes referring to unsuccessful ones have a background that prints in gray.

   The box related to a regular e-mail that is received by the REM Recipient's REM-MD has a hatched background.

2) One REM-MD Message MAY refer to another REM-MD Message referring in turn to the final Original Message to be downloaded, therefore REM-MD Message Delivery (Event D.1) and REM Object download (Event E.4) can be iterated.

3) Events related to servers external to the REM lie on a light gray background.

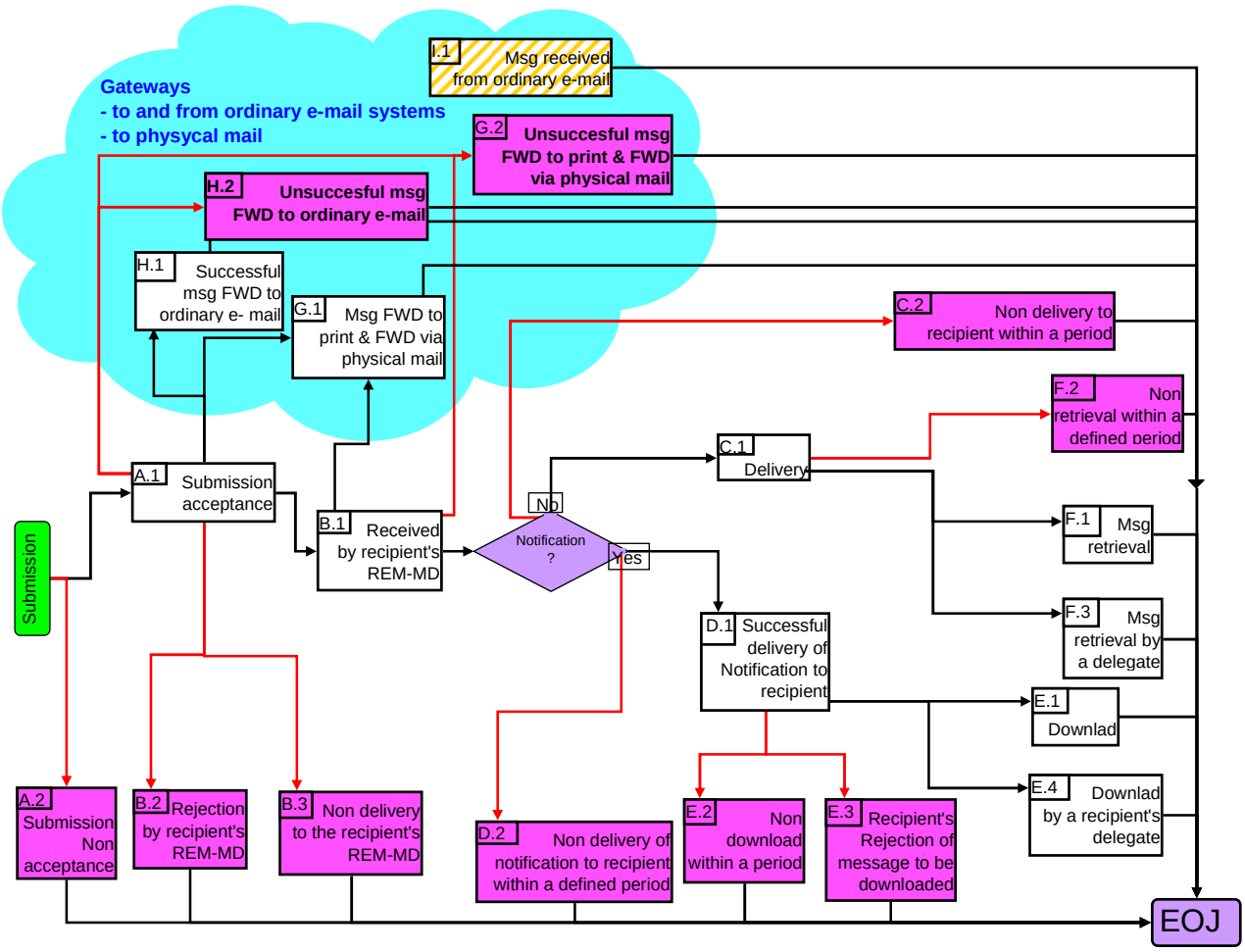


Figure A.2: REM Events flow

Annex B (informative): Bibliography

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

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

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

W3C Recommendation: "XML Signature Syntax and Processing".

IETF RFC 2449 (1998): "POP3 Extension Mechanism".

IETF RFC 2061 (1996): "IMAP4 Compatibility with IMAP2bis".

IETF RFC 2971 (2000): "IMAP4 ID extension".

IETF RFC 3501 (2003): "Internet Message Access Protocol - Version 4rev1".

IETF RFC 2595 (1999): "Using TLS with IMAP, POP3 and ACAP".

IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".

IETF RFC 4954 (2007): "SMTP Service Extension for Authentication".

IETF RFC 2821 (2001): "Simple Mail Transfer Protocol".

IETF RFC 2822 (2001): "Internet Message Format".

History

Document history		
V1.1.1	October 2008	Publication