ETSI TS 102 640-4 V2.1.2 (2011-09)

Technical Specification

Electronic Signatures and Infrastructures (ESI);
Registered Electronic Mail (REM);
Part 4: REM-MD Conformance Profiles

Reference

RTS/ESI-000071-4

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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://ipr.etsi.org).

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 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

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. At the time of writing the present document, in some European Union Member States (Italy, Belgium, etc.) regulation(s) and application(s) are being developed, if not 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 document 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 document assumes the usage of at least an Advanced Electronic Signature, with the meaning of article 2(2) of EU Directive 1999/93/EC [i.7] issued with a Secure Signature Creation Device, with the meaning of article 2(6) of the same Directive.

The summarised scope of each part and sub-part can be found in part 1 [1] of this multi-part deliverable.

1 Scope

The present document specifies two levels of conformance requirements:

- Basic Conformance Profile that indicates the minimum set of mandatory requirements that are to be met by any REM-MD that claims to be conformant with TS 102 640-1 [1], TS 102 640-2 [2] and TS 102 640-3 [3]; and

- Advanced Conformance Profile that includes a set of voluntary additional requirements to the Basic Conformance Profile for enhanced security and advanced evidential services.

It should be emphasize that an organization claiming compliance with TS 102 640-1 [1], TS 102 640-2 [2] and TS 102 640-3 [3] is only expected to fully comply with the mandatory requirements contained in the Basic Conformance Profile.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

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 necessary for the application of the present document.

[1] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[2] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM".

[3] ETSI TS 102 640-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains".

[4] ISO/IEC 27002:2005: "Information technology - Security techniques - Code of practice for information security management".

[5] ETSI TS 101 862: "Qualified Certificate profile".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IETF RFC 1305: "Network Time Protocol (Version 3) Specification, Implementation and Analysis".

[i.2] ETSI TS 102 640-5: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles".

[i.3] ETSI TS 102 640-6-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 1: REM-MD UPU PReM Interoperability Profile".

[i.4] ETSI TS 102 640-6-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 2: REM-MD BUSDOX Interoperability Profile".

[i.5] ETSI TS 102 640-6-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 3: REM-MD SOAP Binding Profile".

[i.6] ISO/IEC 27001:2005: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

3 Definitions, abbreviations and notations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 640-1 [1] apply.

Throughout the present document a number of verbal forms are used, whose meaning is defined below:

- **Shall, shall not:** indicate requirements strictly to be followed in order to conform to the present document and from which no deviation is permitted.
- **Should, should not:** indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.
- **May, need not:** indicate a course of action permissible within the limits of the present document.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 640-1 [1] apply.

3.3 Notations

All the requirements will be defined in tabular form.

Table 1: Requirements template

Nº	[Element]	TS reference	Requirement	Implementation guidance	Notes

Column **Nº** will identify a unique number for the requirements. This number will start from 1 in each clause. The eventual references to it would also include the clause number to avoid any ambiguity.

Column **[Element]** will identify the element the requirement applies to. Elements include architectural elements (clauses 4.1 and 4.4), management element (clause 4.2), roles (clauses 4.3 and 5.4), interfaces (clauses 4.5 and 5.2), Evidence (clauses 4.6 and 5.5), Information Security Management elements (clause 4.7), Security Controls (clause 4.7), REM-PD related elements and Information security management system elements (clause 5.6). Tables in the aforementioned clauses have, in consequence, different headers for this column.

Column **TS Reference** will reference the relevant clause of the standard where the element is defined. The reference is to TS 102 640-1 [1], TS 102 640-2 [2] or TS 102 640-3 [3] except where explicitly indicated otherwise.

Column **Requirement** will contain an identifier, as defined in table 2.

Table 2: Optionality

Identifier	Requirement to implement
M	REM-MD **shall** implement the element
R	REM-MD **should** implement the element
O	REM-MD **may** implement the element

Column **Implementation guidance** will contain guidance explaining how to implement the identified requirement. It is intended either to explain how the requirement is implemented or to.

Column **Notes** will include explanatory and additional information.

4 Basic Profile Requirements

4.1 Basic Elements

Table 3 shows the mandatory architectural elements that shall be present in the logical model of a Registered Electronic Mail service.

Table 3

Nº	Architectural Element	TS reference	Requirement	Implementation guidance	Notes
1	REM-MD	4.1	M		see note 1
2	REM Sender	4.1	M		see note 2
3	REM Recipient	4.1	M		
4	REM-UA	4.1	M		
5	Evidence	4.1	M		see note 3

NOTE 1: The REM Sender has access to the REM-MD services through a User Agent.
NOTE 2: The recipient accesses also the REM-MD services through a User Agent.
NOTE 3: In addition to transport services as provided by other 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).

4.2 REM-MD Management

Table 4 shows the minimum set of requirements for management of a REM-MD and REM-PD.

Table 4

Nº	Management elements	TS reference	Requirement	Implementation guidance	Notes
1	Compliance to rules and procedures	4	M	a)	
2	Documenting procedures	4	M	b)	
3	Provision of information by REM-PD	4	M	c)	see note

NOTE: 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 organizations.

Implementation guidance:

a) The REM-MD **shall** be managed in compliance of rules and procedures ensuring abidance by the regulations governing the relevant REM Policy Domain (company rules, contractual obligations, and/or domestic and international law s and regulations applicable) in order to provide, where applicable, legal validity of REM-Dispatches, REM-MD Messages and REM-MD Evidence.

b) The REM-procedures **shall** be documented in compliance of rules and procedures ensuring abidance by the regulations governing the relevant REM Policy Domain (company rules, contractual obligations, and/or domestic and international law s and regulations applicable) in order to provide, where applicable, legal validity of REM-Dispatches, REM-MD Messages and REM-MD Evidence.

c) The REM-PD management system **shall** provide transparent information to the users on what REM-MD are recognised as compliant with the REM-PD rules.

4.3 Roles

Table 5 shows the list of roles that are mandatory in a REM system.

Table 5

Nº	Role	TS reference	Requirement	Implementation guidance	Notes
1	REM-MD Message Transfer Agent	4.3	M	a)	
2	REM Message Store	4.3	M	b)	
3	REM-MD Evidence Provider	4.3	M		
4	Certification Authority (CA)	4.3	M	c)	

Implementation guidance:

a) The REM-MD Transfer Agents **shall** make use of secure channels to exchange REM Objects with other Transfer Agents and with end users.

b) A REM Message Store **shall** be allocated to the REM Senders and REM Recipients and **shall** be securely accessible by REM Sender and REM Recipients respectively to retrieve REM Objects addressed to them.

c) This role **shall not** be in sourced.

4.4 Authentication

Table 6 shows mandatory requirements on authentication in a REM system.

Table 6

Nº	Architectural element	TS reference	Requirement	Implementation guidance	Notes
1	REM Sender	6.3	M	a)	see note
2	REM Recipient	6.3	M	b)	see note
NOTE: Sender(s) and Recipient(s) requires authentication, hence providing a mechanism for REM system to provide Proof of Sent and Proof of Delivery. Since the fundament principle of REM is to deliver message from the sender to the recipient with reliability comparable with physical register mail, the sender need to be assured that the message or the letter is securely delivered to a person whom he or she would like the message to be delivered to, therefore the authentication of identity of recipient is essential. In addition, having legal support for REM operations are also critical, so that the ability to provide legally recognized Evidence will make a difference between ordinary electronic mail and REM.					

Implementation guidance:

a) REM Senders **shall** authenticate to the relevant REM-Management Domains (REM-MDs), but the choice of the authentication mechanism is left to the specific REM-MD.

b) To receive REM Objects addressed to him the REM Recipient **shall** authenticate to the relevant REM-MD, but the choice of the authentication mechanism is left to the specific REM-MD.

4.5 Interfaces and protocols

Table 7 shows the list of mandatory interfaces in a REM system.

Table 7

Nº	Interface	TS reference	Requirement	Implementation guidance	Notes
1	REM-MD Sender Message Submission Interface	5	M	a)	see note
2	REM-MD Sender/Recipient Message Store Retrieval Interfaces	5	M	b)	
3	REM-MD Repository Retrieval Interface	5	M	c)	
NOTE: SMTP is recommended for granting a common ground to users willing to switch between providers. Nothing prevents from providing a web-mail interface in parallel with or in place of the SMTP interface.					

Implementation guidance:

a) REM Objects **should** be submitted protected (e.g. by using SMTP with TLS/SSL) through this interface. REM Senders **may** authenticate using passwords if protected and only used with an authenticated server (e.g. using TLS/SSL).

b) REM Objects **should** be retrieved protected (e.g. using pop3 or imap with TLS/SSL) through this interface.

c) REM Objects or REM-MD Evidence **should** be retrieved protected (e.g. using HTTP or FTP using a URL with TLS/SSL) through this interface.

4.6 Evidence

Table 8 shows the list of mandatory Evidence to be generated in a REM system.

Table 8

Nº	Evidence	TS reference	Requirement	Implementation guidance	Notes
1	REM-MD Evidence of Submission acceptance	6.2.1 - A 1)	M		see note 1
2	REM-MD Evidence of Submission non acceptance	6.2.1 - A 2)	M		see note 1
3	REM-MD Evidence of Delivery	6.2.3 - C 1)	M (in S&F mode of operation)		see note 2
4	REM-MD Evidence of Non delivery within a given retention period	6.2.3 - C 2)	M (in S&F mode of operation)		see note 2
5	REM-MD Evidence of Delivery to the REM Recipient's mailbox of a reference to REM-MD Repository that a REM Object is available for downloading	6.2.3 - D 1)	M in S&N style of operation		see note 2

Nº	Evidence	TS reference	Requirement	Implementation guidance	Notes
6	REM-MD Evidence of 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	6.2.3 - D 2)	M in S&N style of operation		see note 2
7	REM-MD Evidence of Download	6.2.3 - E 1)	M in S&N style of operation		see note 2
8	REM-MD Evidence of Non download within a given retention period	6.2.3 - E 2)	M in S&N style of operation		see note 2
NOTE 1: This is an evidence related to REM Sender's REM-MD. NOTE 2: This is an evidence related to REM Recipient.					

4.7 Information Security

Table 9 shows the list of mandatory requirements, related to Information Security management (ISM in table 9), in a REM system.

Table 9

Nº	ISM Element	TS reference	Requirement	Implementation guidance	Notes
1	Risk assessment implementation	5.2	M	a)	see note 1
2	Documentation production	5.2	M	b)	
3	Physical security	5.2	M	c)	
4	Time synchronization	5.6	M	d)	
5	Access Control	5.7	M	e)	
6	Policies for management of Information security incident	5.9	M		see note 2
7	Disaster recovery programme	5.9	M		see note 3
NOTE 1: A set of security controls **may** be found in ISO/IEC 27002 [4]. NOTE 2: A Service Level Agreement (SLA) is recommended to be made available to, and explicitly accepted by, all subscribers. At least its highlights are published in the publicly available parts of the REM Policy. This SLA is recommended to be in writing and in readily understandable language. The way the SLA is provided to REM subscribers is to be specified in the REM Policy. NOTE 3: A managed process is recommended to be developed and maintained for REM-MD business continuity addressing the information security requirements needed for the REM-MD business continuity.					

Implementation guidance:

a) Security controls **shall** be implemented based on a risk assessment to ensure integrity, availability and confidentiality of REM-MD information.

b) Documentation **shall** be implemented to ensure that the all relevant REM-MD information (as messages, Evidence, logs, etc.) is securely created, transmitted, delivered and stored.

c) Physical security **shall** be implemented to ensure that the all relevant REM-MD information (as messages, Evidence, logs, etc.

d) Time **shall** be implemented to ensure that the all relevant REM-MD elements are synchronized.

e) Access control policy **shall** be in place, based on best practices as in ISO/IEC 27002 [4] ensuring that only authorised personnel **may**:

   1) access the REM-MD system logical and physical components, network included;

   2) access the REM-MD facilities, including those related to the network;

3) send and access REM Objects.

Table 10 shows the list of additional mandatory REM-specific security controls, within the context of the ISO/IEC 27002 [4] requirements specified in table 9.

Table 10

Nº	Security Control	TS reference	Requirement	Implementation guidance	Notes
8	QC Statements when signature is supported by Qualified Certificate	6.4.1	M	f) g)	
9	Independence between the line of operations of the CA supporting REM-MD signatures and of the REM-MD itself	6.4.2	M	h)	
10	Protection of Private Signing Key	6.4.3	M		
11	Maintenance of REM-MD Evidence and REM-MD Envelopes over storage period	6.5	M		see note 1
12	Records Retention and Destruction	6.6	M	i)	see note 2
NOTE 1: One single Organisation **may** operate both a REM-MD and a long term archival service provided that these lines of operations report directly either the CEO, or to an equivalent role, or to different Executives that in turn report directly to the CEO. NOTE 2: By "secure deletion" it is intended a procedure that, based on state of the art technology, ensures that the deleted data cannot be recovered.					

Implementation guidance:

a) When the certificate supporting the signature is a Qualified Certificate it **shall** include the extensions "esi4-qcStatement-1" and "esi4-qcStatement-4" as defined in TS 101 862 [5], clauses 5.2.1 and 5.2.4.

b) Key roles to the security of the REM archival service **shall** be undertaken by personnel not concerned with the operation of the rest of the REM, and be managed separate from the REM management structure.

c) Independence between the line of operations of the CA supporting REM-MD signatures and of the REM-MD itself **shall** be documented.

d) When storage media cannot be physically destroyed then data **shall** be deleted using secure data deletion procedures.

5 Advanced Profile Requirements

5.1 General

The Advanced Profile establishes voluntary enhanced requirements that may be satisfied in all or in part. It includes some further REM-MD Evidence and security controls that enhance REM-MD's information security and legal reliability.

It is strongly recommended that REM-MD organizations comply with ISO/IEC 27002 [4] as stated in TS 102 640-3 [3].

5.2 Interfaces and protocols

Table 11 lists the list of recommended interfaces that would be added to the mandatory interfaces listed in clause 4.5. Table 11 incorporates implementation guidance on protocols recommended for these interfaces.

Table 11

Nº	Interface/protocols	TS reference	Requirement	Implementation guidance	Notes
1	Non REM Relay Interface.	5	R	a)	
2	REM Object Relay Interface.	5	R	b)	
3	Third Party Evidence Retrieval Interface	5	R	c)	
4	REM-MD MTA exchange through secure channels		R		
5	REM-MD Transfer Agents should make use of secure channels to exchange REM Objects with other Transfer Agents and with end users	5	R		

Implementation guidance:

a) S/MIME over SMTP **should** be used for relaying REM Objects through the non REM Relay Interface.

b) A recognised standard protocol which authenticates the origin of the REM Object (e.g. S/MIME over SMTP) **should** be used when REM-MDs interact through the REM Object Relay Interface.

c) This interface **should** be implemented when there is the requirement that a third party may gain access to the REM-MD Evidence.

5.3 REM-PD related elements

Table 12 lists recommended and optional requirements on elements related with REM-PD.

Table 12

Nº	REM-PD related Element	TS reference	Requirement	Implementation guidance	Notes
1	Multiple REM-MDs in the same REM-PD		O	a)	
2	Trust List		R	b)	

Implementation guidance:

a) If a REM-PD is formed by more than one REM-MD then the list of its REM-MDs members **should** be made available within the REM-PD.

b) The Trust List **should** be made available outside the REM-PD.

5.4 Roles

Table 13 lists additional recommended and optional roles within a REM system.

Table 13

Nº	Role	TS reference	Requirement	Implementation guidance	Notes
1	Message Archive		R		
2	REM-MD Repository		O		
3	REM-MD Evidence Verifier		O		
4	REM-MD Message Gateway		O		
5	Signature Creation Server		O		
6	Time-Stamping Authority (TSA)		R	a)	
7	Long Term Storage		R		

Implementation guidance:

a) Network Time Protocol - RFC 1305 [i.1] - specifications may be used.

5.5 Evidence

All the following REM-MD Evidence are issued according to the TS 102 640-2 [2] provisions and to the subsequent indications.

An advanced REM-MD **should** consider implementing the REM-MD Evidence contained in this table in addition to those indicated in clause 4.6.

Table 14

Nº	Evidence	TS reference	Requirement	Implementation guidance	Notes
1	REM Object acceptance by the REM Recipient's REM-MD	6.2.2 - B 1)	R	a)	see note 1
2	Evidence REM Object rejection by the REM Recipient's REM-MD	6.2.2 - B 2)	R	a)	see note 2
3	Non delivery within a given time period of the REM Object to the REM Recipient's REM-MD	6.2.2 - B 3)	R		see note 2
4	Rejection by the REM Recipient of the REM Object to be downloaded	6.2.3 - E 3)	R		see note 2
5	Download by an entity delegated by the REM Recipient	6.2.3 - E 4	R		see note 2
6	Retrieval	6.2.3 - F 1)	R		see note 2
7	Non retrieval within a given period	6.2.3 - F 2)	R		see note 2
8	REM Object retrieval by an entity delegated by the REM Recipient	6.2.3 - F 3)	R		see note 2
9	Printing	6.2.4 - G 1)	R		see note 2
10	The submission to a printing system of the Original Message to be subsequently sent via physical registered mail was unsuccessful	6.2.4 - G 2)	R		see note 3
11	The REM Object was successfully forwarded to a regular e-mail service	6.2.4 - H 1)	R		see note 3

Nº	Evidence	TS reference	Requirement	Implementation guidance	Notes
12	The REM Object forwarding to regular e-mail was unsuccessful	6.2.4 - H 2)	R		see note 3
13	Non REM origin	6.2.4 - I	R		see note 3
NOTE 1: Evidence related to the REM Recipient's REM-MD. NOTE 2: Evidence related to the REM Recipient. NOTE 3: Evidence related to connections with outside the REM-MD.					

Implementation guidance

a) This Evidence **should** be mandatory if:

- no opposite provision is explicitly specified in the applicable legislation or REM-PD policy;
- no previous opposite agreement exists between the involved REM-MDs.

The applicable REM-PD policy **should** indicate if this evidence type **should** be implemented/not implemented. Alternatively such provision may be specified in a bilateral agreement between the REM-MD at issue and some other REM-MD.

Where such agreement or REM-PD policy provision does not make mandatory this evidence and the subsequent one it **should** specify one of the following:

- the sender's REM-MD will assume that one REM-MD Envelope (be it a REM-MD Message or a REM Dispatch) has been rejected by the recipient's REM-MD if no contrary indication is received within a predefined time period;
- the sender's REM-MD will assume that one REM-MD Envelope has been accepted by the recipient's REM-MD if no contrary indication is received within a predefined time period. Alternative conditions **may** be specified in the above agreement, provided that the issue is exhaustively dealt with.

5.6 Information security management system

In addition to ISO/IEC 27002 [4] controls, an advanced REM-MD **should** consider implementing also the specific security controls contained in table 15.

Table 15

Nº	ISMC	TS 102 640-3 [3]	Requirement	Implementation guidance	Notes
1	REM-MD interconnection	5.2 b)	R	a)	see note
2	REM Sender/REM Recipient Authentication	6.3	O	b)	
3	Class of Electronic Signature	6.4.1	O	c)	
4	Key signature	6.4.3	R	d)	
NOTE: An interchange agreement is not necessary where the REM Policy covers requirements for interconnection.					

Implementation guidance:

a) When interconnecting with other REM-MD, interconnection agreement should be defined between REM-MDs as specified in clause 6.2 of the present document.

b) In certain cases the relevant REM Policy **may** require REM-MDs to adopt specific REM Sender/REM Recipient Authentication mechanisms when REM Dispatches and/or REM-MD Messages are to be exchanged with external REM-MDs or REM-PDs.

c) In certain cases the relevant REM Policy **may** require to adopt specific Classes of Electronic Signatures when REM Dispatches and/or REM-MD Messages are to be exchanged with external REM-MDs or REM-PDs.

d) The key used to sign REM-MD Evidence and REM-MD Envelopes shall be held and used within a secure cryptographic device.

History

Document history		
V2.1.1	January 2010	Publication
V2.1.2	September 2011	Publication