ETSI TS 102 640-3 V1.1.1 (2008-10)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 3: Information Security Policy Requirements for REM Management Domains

Reference

DTS/ESI-000052-3

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 3 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 [4].

1 Scope

The present document specifies requirements on the security of a Registered E-Mail Management Domain (REM-MD). These requirements are based on the REM-MD operating an Information Security Management System as specified in ISO/IEC 27001 [1].

Requirements relating to the handling of messages (e.g. message transfer or storage) which do not impact on the REM related evidence are outside the scope of the present document.

The present document uses the concepts and models defined in TS 102 640-1 [i.1].

The present document considers the policy requirements applicable to the REM-MD as a whole. It is the responsibility of the management authority for that domain to ensure the requirements of that domain are met including any requirements which impact on external 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 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] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

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

[3] ISO/IEC 27005: "Information technology - Security techniques - Information security risk management".

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

[5] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[6] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[7] CWA 14169: "Secure signature-creation devices "EAL 4+"".

NOTE: CWA 14169 was drafted based on Common Criteria 2.1 which has since been superseded. It is specified in the Common criteria site (http://www.commoncriteriaportal.org/thecc.html): "[omissis] _the 2.* series,_ [is] _to be used until March 2008, and maintenance based in this version during further 18 months, i.e. until September 2009_".

[8] ISO/IEC 15408 (Parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

[9] CEN CWA 14167 (Parts 2 and 4): "Cryptographic module for CSP signing operations with / without backup - Protection profile - CMCSOB PP / CMCSO PP".

[10] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

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

[i.2] 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".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

REM	Registered E-Mail
REM-MD	REM Management Domain
ISMS	Information Security Management System
WORM	Write Once Read Many

4 Information security management systems in REM-MDs

4.1 Goal/ISMS introduction

Information, like other organization assets, is an essential contributor to an organization's business. Regardless of the form or functionality of the information, or the means by which the information is shared or stored, information should always be appropriately protected.

The users of REM-MD services depend on evidence being collected and secured in a trusted manner. Users of a REM-MD need confidence that the information with REM-MD Evidence truly represent the messaging events handled by the REM-MD, and that when issued the REM-MD Evidence is properly secured using electronic signatures. In order to provide this confidence the operation of the REM-MD needs to be properly managed. Therefore, it is essential for an organization to ensure its information security by continuously improving information security management system (ISMS) in accordance with ISO/IEC 27001 [1]. In addition, as the REM-MD needs to meet specific security objective relating to authenticity and integrity of the REM-MD Evidence and the application of Electronic Signature, specific policy objectives and controls need to be applied to address known threats to such objectives.

REM-MDs and their information systems and networks are faced with general security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, unauthorized modification of evidence and leakage of personal message information. These threats may originate from inside or outside the REM-MD. Once information security is violated, for example by unauthorized modification to REM-MD Evidence, user confidence in the REM-MD will suffer major damage. Furthermore, the resulting impact on the user's business and potentially a critical element of national infrastructure (secure messaging services) could be significant.

4.1.1 Information Security Policy vs REM Policy

An Information Security Policy is a statement of policy which provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. It is one of the fundamental components of an Information Security Management System based on ISO/IEC 27001 [1]. An Information Security Policy is concerned with information security rather than the general requirements of REM. A REM-MD should have its own Information Security Policy.

A REM Policy is a set of rules (e.g. legal, company policy or agreement) enforced for the provision of REM Services. It is aimed at rules regarding the general operation of REM. A REM Policy may include requirements on the security of REM Services. An identified REM Policy may apply to one or more REM-MDs.

4.2 Information asset to be protected

The prime information asset of the REM-MD is REM-MD Evidence, and the information collected to form REM-MD Evidence. The integrity of REM-MD Evidence and the information collected, and the data origin authentication of REM-MD Evidence must be assured. The privacy of REM-MD Evidence is also of some concern.

A second information asset of the REM-MD are the different forms of REM Object. As well as assuring the integrity of REM-MD Messages and REM-MD Dispatches, the REM-MD must maintain the privacy of all REM Objects, including information on the flow of REM Messages.

A number of assets will exist in REM-MD which need to be considered in assessing the risks to a REM-MD (see ISO/IEC 27005 [3] for discussion on assets).

4.3 Establishment of information security management

4.3.1 How to establish security requirements

In considering the security requirements for a REM-MD particular attention needs to be made on maintaining the integrity of the REM-MD systems and the information it holds.

In addition, the privacy of the messages and related evidence needs to be protected to meet the requirements of Data Protection legislation.

For general guidance on establishing security requirements and assessing security risks see ISO/IEC 27005 [3].

4.3.2 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

For general guidance on establishing security requirements and assessing security risks see ISO/IEC 27005 [3].

4.3.3 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level.

The present document provides recommended controls for REM-MDs based on the controls recommended in ISO/IEC 27002 [2] adapted to meet the requirements of REM.

The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to REM-MDs, and should also be subject to all relevant national and international legislation and regulations.

4.3.4 Critical success factors

ISO/IEC 27002 [2], clause 0.7 applies.

5 Application of ISO/IEC 27002 Controls and Objectives

The controls specified in ISO/IEC 27002 [2] shall be applied by an ISMS conforming to ISO/IEC 27001 [1] taking into account the following.

5.1 Security Policy

Controls under clause 5 from ISO/IEC 27002 [2] apply.

The REM-MD shall establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System as specified in ISO/IEC 27001 [1], applying the controls identified in this clause and, as determined through ISMS, ISO/IEC 27002 [2], taking into account the additional points identified in clause 6.

5.2 Organization of information security

Controls under clause 6.1 from ISO/IEC 27002 [2] apply.

Controls under clauses 6.2.1 and 6.2.2 from ISO/IEC 27002 [2] apply.

In the context of clause 6.2 of ISO/IEC 27002 [2]:

a) In order to maintain security with external parties the REM-MD shall also make available a REM Practices Statement to REM Senders, REM Recipients and other third parties using the REM-MD services as specified in clause 6.1 of the present document.

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

5.3 Asset management

Controls under clause 7 from ISO/IEC 27002 [2] apply, in particular for REM-MD Evidence and those assets forming components of REM-MD Evidence as well as REM Objects.

5.4 Human resources security

Controls under clause 8 from ISO/IEC 27002 [2] apply.

5.5 Physical and environmental security

Controls under clause 9 from ISO/IEC 27002 [2]apply.

5.6 Communications and operations management

Controls under clause 10 from ISO/IEC 27002 [2] apply. In particular, clocks of all REM-MD systems which impact the time used in audit records and REM-MD Evidence shall be synchronized with UTC (if required with local offset which shall be recorded in the REM Practice statement) within 1 minute.

5.7 Access control

Controls under clause 11 from ISO/IEC 27002 [2] apply.

In particular, REM Senders and REM Recipients shall be authenticated as specified in clause 6.3 of the present document.

5.8 Security requirements of information systems

Controls under clause 12 from ISO/IEC 27002 [2] apply.

In particular, in relation to cryptographic controls specified in clause 12.3 of ISO/IEC 27002 [2], electronic signatures shall be applied as specified in clause 6.4.

5.9 Information security incident management

Controls under clause 13 from ISO/IEC 27002 [2] apply.

5.10 Business continuity management

Controls under clause 14 from ISO/IEC 27002 [2] apply.

5.11 Compliance

Controls under clause 15 from ISO/IEC 27002 [2] apply.

In particular:

a) in the context of clause 15.1.3 the integrity of REM-MD Evidence shall be preserved as specified in clause 6.5;

b) in the context of clause 15.1.3 records shall be destroyed as specified in clause 6.6;

c) in the context of clause 15.2 any REM Policy applicable to the REM-MD shall be applied.

6 Further Requirements

The following controls shall be applied within the context of the ISO/IEC 27002 [2] requirements as specified above.

6.1 REM Practice Statement

The REM Practice Statement is a statement of the practices employed in providing REM services meeting the policy requirements specified in the present document.

The REM Practice statement shall include as applicable:

a) The country under whose legal system the REM-MD operates and other applicable legal requirements.

b) Reference to REM Policy or other legal or policy requirements to which the REM-MD conforms.

c) Details of any certification of conformance, government accreditation or other form of external audit against the requirements specified in the present document.

d) Information on how the requirements specified in the present document are implemented, including:

   i) a statement of applicability of the ISO/IEC 27002 [2] controls taking into account the particular requirements specified in the present document;

   ii) whether Advanced signatures are supported by an SSCD and / or Qualified Certificate in accordance with Directive 1999/93/EC [4];

   iii) the level of authentication required by REM Senders and REM Recipients (see clause 6.3);

   iv) the period of time for which records are kept.

e) Obligations to be met by the REM Sender, including:

   i) protect any keys, password or other objects used to authenticate the REM Recipient;

   ii) any obligations to maintain REM-MD Evidence if not kept by the REM-MD.

f) Obligations to be met by the REM Recipient, including:

   i) protect any keys, password or other objects used to authenticate the REM Recipient;

   ii) any obligations to maintain REM-MD Evidence if not kept by the REM-MD.

g) Obligations to be met by any party relying on REM-MD Evidence, including:

   i) verify the validity of REM-MD Evidence; this includes:

      - verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying parties in the related CA's Certificate Policy and / or Certificate Practice Statement; and

NOTE: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay in disseminating revocation status information. Thus, the verifier may need to await the next CRL, or even one following that, to be assured any relevant revocation request has been processed.

      - take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate itself or in the terms and conditions supplied by the certificate issuing CA;

   ii) apply security measures as notified by the REM-MD when accessing the REM-MD to obtain REM-MD Evidence;

   iii) any obligations to maintain REM-MD Evidence if not kept by the REM-MD.

6.2 REM Interconnection Statement

The REM Interconnection statement is an agreement between REM-MDs or a statement of policy from an Authority recognized by both REM-MDs defining the controls to be applied to protect data exchanged between the REM-MDs.

6.3 REM Sender / REM Recipient Authentication

REM Senders and REM Recipients, as identified in REM-MD Evidence, shall be authenticated by either:

a) using basic authentication mechanisms such as passwords, or

b) using enhanced authentication such two factor authentication mechanisms linked to a one time password, or

c) using advanced electronic signatures, or

d) using advanced electronic signatures with Secure Signature Creation Devices (as defined in Directive 1999/93/EC [4]) or equivalent secure cryptographic device;

e) using advanced electronic signatures with Secure Signature Creation Devices and Qualified Certificates (as defined in Directive 1999/93/EC [4]).

The form of authentication used shall be documented in the REM Practice Statement.

NOTE: See also TS 102 640-2 [i.2], clause on "REM Sender / Recipient authentication details".

6.4 Electronic Signatures

6.4.1 Class of Electronic Signature

Objective: To employ a class of electronic signature that assures the authenticity and integrity, and where applicable commitment to content, over the lifetime of REM-MD Evidence and REM-MD Envelopes.

The signature on REM-MD Evidence and REM Envelopes shall be at least an Advanced Electronic Signature, as defined in Directive 1999/93/EC [4]. The signature may be created using a Secure Signature Creation Devices and / or Qualified Certificates (as defined in Directive 1999/93/EC [4]).

The form of signature used shall be document in the REM Practice Statement.

6.4.2 Certification

Objective: To obtain certificates from authority who can reliably certify public keys and maintain revocation status information.

REM-MD Evidence and REM Envelope signatures shall be supported by either:

a) Certificates issued by CAs that operate under certificate policies as per TS 102 042 [5] (NCP+ type) or practices that are nationally recognized as being sufficiently reliable for the purposes of signing fiscally relevant data, or

b) Qualified certificates issued by CAs that operate under qualified certificate policies as per TS 101 456 [6] (include requirements for the use of SSCD**)** or practices that are nationally recognized for issuing qualified certificates.

NOTE: In a number of countries qualified certificates can only be issued to natural persons and hence would be inappropriate for signing by the REM organization.

The operation of the CA supporting REM-MD signatures shall be independent of the REM-MD.

6.4.3 Protection of Private Signing Key

Objective: To ensure that the private signing key used to sign REM-MD Evidence and REM-MD Envelopes is generated and is kept secure in controlled circumstances.

The key used to sign REM-MD Evidence and REM-MD Envelopes shall be held and used within a secure cryptographic device which:

a) meets the requirements identified in FIPS PUB 140-2 [10] level 3 or higher; or

b) meets the requirements identified in the CEN Workshop Agreement CWA 14169 [7]; or

c) meets the requirements identified in the CEN Workshop Agreement CWA 14167-2 or 14167-4 [9]; or

NOTE: Section 3 "TOE Security Environment" of these documents specify requirements on the environment in which these devices are to be kept.

d) is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or

e) it is assured to any comparable criteria recognized in the specific EU Member State.

6.5 Maintenance of REM-MD Evidence and REM-MD Envelopes over storage period

Objective: To ensure that the electronic signatures against REM-MD Evidence and REM-MD Envelopes are maintained such that their validity can be verified for period that it is stated in the REM Practice Statement that REM-MD Evidence is retained.

This may be achieved either by:

a) Employing Cryptographic and Media controls whereby:

    i) all the information required to perform the signature verification, (e.g. certificate path from a known trust point, e.g. root CA and revocation information), and a trusted indicator (e.g. time-stamp) of the time when that signature existed and was valid shall be stored for the same time as the related signed document; and

    ii) if the signed documents are to be stored for a period which is longer than the one for which the strength of the cryptographic algorithms employed can be assured, then additional integrity mechanisms shall be applied to the signed document and verification information. This may be achieved for example by employing archive time-stamps or maintaining the documents in write once read many (WORM) media which cannot be modified once written.

b) Employing an independent third party (e.g. Notary) which is trusted to maintain the integrity of signed evidence.

6.6 Records Retention and Destruction

Records shall be kept relating to the provision of REM services, including audit logs and REM-MD Evidence, for the period required to support local law and any agreement with REM Users, by means that maintains their authenticity and integrity over the required period. In particular, REM Sender's and REM Recipient's personal data must be destroyed when no longer required, unless differently agreed upon with the users or required by the applicable legislation.

Annex A (informative): Bibliography

ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

History

Document history		
V1.1.1	October 2008	Publication