

TECHNICAL SPECIFICATION



**Framework for energy market communications –
Part 503: Market data exchanges guidelines for the IEC 62325-351 profile**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE

XD

ICS 33.200

ISBN 978-2-8322-1368-1

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms and definitions	11
4 High level concepts	12
4.1 What is MADES intended for?	12
4.2 General overview	13
4.3 Message delivery and transparency	14
4.3.1 Message delivery.....	14
4.3.2 Transparency.....	14
4.4 Security and reliability.....	15
4.5 Main components.....	16
4.6 Distributed architecture.....	17
4.7 Components' exposed interfaces	18
4.8 Security features.....	18
4.8.1 Overview	18
4.8.2 Transport-layer security.....	19
4.8.3 Message-level security.....	20
4.8.4 Non repudiation.....	21
5 Components' functions	22
5.1 Routing messages	22
5.2 Component and message unique identification (ID).....	23
5.3 Business-type of a business-message	23
5.4 Delivery-status of a business-message	23
5.5 Communication between components	25
5.5.1 Principle	25
5.5.2 Establishing a secured communication channel between two components.....	25
5.5.3 Token authentication of the client component	26
5.5.4 Request authorisation.....	26
5.5.5 Request/Reply validation	26
5.6 Storing messages in components.....	27
5.7 Lifecycle of a message state within a component	27
5.8 Transferring a message between two components (Handshake)	29
5.9 Accepting a message.....	30
5.10 Event management.....	31
5.10.1 Acknowledgements.....	31
5.10.2 Notifying events.....	32
5.10.3 Lifecycle of an acknowledgement	34
5.10.4 Processing a transferred acknowledgement.....	34
5.11 Message expiration.....	35
5.11.1 Principle	35
5.11.2 Setting the expiration time of a message:	35
5.11.3 Looking for the expired messages:	35
5.12 Checking the connectivity between two endpoints (Tracing-messages)	35
5.13 Ordering the messages (Priority).....	36

5.14	Endpoint	36
5.14.1	Endpoint functions	36
5.14.2	Compression	37
5.14.3	Signing	38
5.14.4	Encryption	39
5.15	Node	41
5.15.1	Node functions	41
5.15.2	Synchronizing directory with other nodes	41
5.15.3	Updating the synchronization nodes' list	42
5.16	Certificates and directory management	43
5.16.1	Definitions and principles	43
5.16.2	Certificates: Format and unique ID	44
5.16.3	Used certificates and issuers (CAs)	44
5.16.4	Directory services	46
5.16.5	Caching directory data	46
5.16.6	Trusting the certificates of others components	47
5.16.7	Renewing the expired certificates	47
5.16.8	Revoking a certificate	48
6	Managing the version of the MADES specification	49
6.1	Issues and principles	49
6.1.1	General	49
6.1.2	Rolling out a new version (Mversion and N-compliance)	49
6.1.3	Service compatibility	49
6.1.4	Message compatibility	50
6.1.5	Interface with BAS	50
6.2	Using the correct version for services and messages	51
6.2.1	Node synchronization and authentication	51
6.2.2	Directory services and Network acceptance	52
6.2.3	Messaging services	53
6.2.4	Which version to use to send a message?	53
7	Interfaces and services	55
7.1	Overview	55
7.1.1	General	55
7.1.2	Error Codes	55
7.1.3	Types for Time	55
7.2	Endpoint interface	56
7.2.1	Overview	56
7.2.2	Services	56
7.2.3	File System Shared Folders (FSSF)	60
7.3	Node interface	62
7.3.1	Overview	62
7.3.2	Authentication service	63
7.3.3	Messaging Services	64
7.3.4	Directory services	67
7.3.5	Node Synchronization interface	70
7.4	Format of the node-list file	71
7.5	Typed Elements used by the interfaces	72
7.6	Description of the services	79
7.6.1	About WSDL and SOAP	79

7.6.2	Endpoint interface.....	79
7.6.3	Node interface	86
7.6.4	XML signature example	100
Figure 1 – MADES overall view.....		12
Figure 2 – MADES scope.....		13
Figure 3 – MADES key features		13
Figure 4 – MADES message delivery overview		14
Figure 5 – MADES security and reliability		15
Figure 6 – MADES components		16
Figure 7 – MADES network distributed architecture		17
Figure 8 – MADES interfaces and services		18
Figure 9 – MADES transport security overview		19
Figure 10 – MADES secure communication initiation		19
Figure 11 – Message signature.....		20
Figure 12 – Message encryption and decryption		20
Figure 13 – Non repudiation.....		21
Figure 14 – Delivery route of a business-message		22
Figure 15 – Reported events during the delivery of a business-message		24
Figure 16 – Lifecycle of the local state of a business-message within a component		28
Figure 17 – Transfer handshake when uploading of a message		29
Figure 18 – Transfer handshake when downloading of a message		30
Figure 19 – Acknowledgements along the route of the business-message		32
Figure 20 – Encryption process.....		40
Figure 21 – A node synchronizes with two other nodes		42
Figure 22 – Certificates and certificate authorities (CAs) for a MADES network		45
Figure 23 – Managing the specification version – node synchronization and authentication.....		51
Figure 24 – Managing the specification version – Directory services		52
Figure 25 – Managing the specification version – Messaging services		53
Figure 26 – Managing the specification version – Which version to use to send a message?		54
Figure 27 – Node interface – Overview		63
Figure 28 – Node interface – Authentication service		63
Figure 29 – Node interface – Messaging services – UploadMessages service.....		65
Figure 30 – Node interface – Messaging services – DownloadMessages service		66
Figure 31 – Node interface – Messaging services – ConfirmDownload service.....		67
Figure 32 – Node interface – Directory services – GetCertificate service		68
Figure 33 – Node interface – Directory services – GetComponent service.....		70
Figure 34 – WSDL 1.1 definitions.....		79
Table 1 – Message delivery status		25
Table 2 – Business message status		28
Table 3 – Accepting a message – Validation checks		31

Table 4 – Characteristics of notified events.....	33
Table 5 – Event characteristics description	34
Table 6 – Acknowledgement state description.....	34
Table 7 – Compression – metadata attributes	38
Table 8 – Signing – metadata attributes	39
Table 9 – Encryption – metadata attributes	40
Table 10 – Consequences of a certificate revocation	48
Table 11 – Service compatibility – Possible changes	50
Table 12 – Which version to use to send a message?	54
Table 13 – Managing the specification version – Rejection conditions.....	54
Table 14 – Interfaces and services – Generic error	55
Table 15 – Interfaces and services – String value for errorCode	55
Table 16 – SendMessage – Service request elements	56
Table 17 – SendMessage – Service response elements.....	57
Table 18 – SendMessage – Additional error elements.....	57
Table 19 – ReceiveMessage – Service request elements.....	57
Table 20 – ReceiveMessage – Service response elements.....	57
Table 21 – ReceiveMessage – Additional error elements.....	58
Table 22 – CheckMessageStatus – Service request elements.....	58
Table 23 – CheckMessageStatus – Service response elements	58
Table 24 – CheckMessageStatus – Additional error elements	58
Table 25 – ConnectivityTest – Service request elements	59
Table 26 – ConnectivityTest – Service response elements.....	59
Table 27 – ConnectivityTest – Additional error elements.....	59
Table 28 – ConfirmReceiveMessage – Service request elements.....	59
Table 29 – ConfirmReceiveMessage – Service response elements	59
Table 30 – ConfirmReceiveMessage – Additional error elements	60
Table 31 – FSSF – Description and filename format.....	61
Table 32 – FSSF – Filename description.....	61
Table 33 – Authentication – Service request elements	64
Table 34 – Authentication – Service response elements	64
Table 35 – UploadMessages – Service request elements.....	65
Table 36 – UploadMessages – Service response elements	65
Table 37 – DownloadMessages – Service request elements	66
Table 38 – DownloadMessages – Service response elements.....	66
Table 39 – ConfirmDownload – Service request elements.....	67
Table 40 – ConfirmDownload – Service response elements	67
Table 41 – SetComponentMversion – Service request elements	68
Table 42 – SetComponentMversion – Service response elements.....	68
Table 43 – GetCertificate – Service request elements.....	69
Table 44 – GetCertificate – Service response elements	69
Table 45 – GetCertificate – Additional conditions	69
Table 46 – GetComponent – Service request elements.....	70

Table 47 – GetComponent – Service response elements	70
Table 48 – GetNodeMversion – Service request elements	70
Table 49 – GetNodeMversion – Service response elements	71
Table 50 – GetAllDirectoryData – Service request elements	71
Table 51 – GetAllDirectoryData – Service response elements	71
Table 52 – Node attributes ordered list	71
Table 53 – AuthenticationToken	72
Table 54 – Certificate	72
Table 55 – CertificateType – string enumeration	72
Table 56 – ComponentCertificate	72
Table 57 – ComponentDescription	73
Table 58 – ComponentInformation	73
Table 59 – ComponentType – string enumeration	73
Table 60 – Endpoint	73
Table 61 – InternalMessage	74
Table 62 – InternalMessageType – string enumeration	75
Table 63 – MessageMetadata	75
Table 64 – MessageProcessor	75
Table 65 – Map	75
Table 66 – MapEntry	76
Table 67 – ValueType (enumeration)	76
Table 68 – MessageState (string enumeration)	76
Table 69 – MessageStatus	76
Table 70 – MessageTraceItem	77
Table 71 – MessageTraceState (string enumeration)	77
Table 72 – NotConfirmedMessageResponse	77
Table 73 – NotUploadedMessageResponse	78
Table 74 – ReceivedMessage	78
Table 75 – RoutingInformation	78
Table 76 – SentMessage	78

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

Part 503: Market data exchanges guidelines for the IEC 62325-351 profile

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC/TS 62325-503, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

DTS	Report on voting
57/1370/DTS	57/1401/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62325 series, published under the general title *Framework for energy market communications*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This Technical Specification is part of the IEC 62325 series which defines protocols for deregulated energy market communications.

The principal objective of the IEC 62325 series is to produce standards which facilitate the integration of market application software developed independently by different vendors into a market management system, between market management systems and market participant systems. This is accomplished by defining message exchanges to enable these applications or systems access to public data and exchange information independent of how such information is represented internally.

The common information model (CIM) specifies the basis for the semantics for the message exchange. The European style market profile specifications that support the European style design electricity markets are defined in IEC 62325-351. These electricity markets are based on the European regulations, and on the concepts of third party access and zonal markets. The IEC 62325-451-n International standards specify the content of the messages exchanged.

The purpose of this technical specification is to provide the guidelines to exchange the above mentioned messages. A European market participant (trader, distribution utilities, etc.) could benefit from a single, common, harmonized and secure platform for message exchange with the European Transmission System Operators (TSOs); thus reducing the cost of building different IT platforms to interface with all the parties involved.

This Technical Specification represents an important step in facilitating parties entering into electricity markets other than their national ones; they could use the same or similar information exchange system to participate in more than one market all over Europe.

This Technical Specification was originally based upon the work of the European Network of Transmission System Operators (ENTSO-E) Working Group EDI.

FRAMEWORK FOR ENERGY MARKET COMMUNICATIONS –

Part 503: Market data exchanges guidelines for the IEC 62325-351 profile

1 Scope

This technical specification is for European electricity markets.

This document specifies a standard for a communication platform which every Transmission System Operator (TSO) in Europe may use to reliably and securely exchange documents for the energy market. Consequently a European market participant (trader, distribution utilities, etc.) could benefit from a single, common, harmonized and secure platform for message exchange with the different TSOs; thus reducing the cost of building different IT platforms to interface with all the parties involved. This also represents an important step in facilitating parties entering into markets other than their national ones.

From now on the acronym “MADES” (Market Data ExchangeS) will be used to designate these Technical Specifications.

MADES is a specification for a decentralized common communication platform based on international IT protocol standards:

- From a business application (BA) perspective, MADES specifies software interfaces to exchange electronic documents with other BAs. Such interfaces mainly provide means to send and receive documents using a so-called “MADES network”. Every step of the delivery process is acknowledged, and the sender can request about the delivery status of a document. This is done through acknowledgement, which are messages returned back to the sender. This makes MADES networks usable for exchanging documents in business processes requiring reliable delivery.
- MADES also specifies all services for the business application (BA); the complexities of recipient localisation, recipient connection status, message routing and security are hidden from the connecting BA. MADES services include directory, authentication, encryption, signing, message tracking, message logging and temporary message storage.

The purpose of MADES is to create a data exchange standard comprised of standard protocols and utilizing IT best practices to create a mechanism for exchanging data over any TCP/IP communication network, in order to facilitate business to business information exchanges as described in IEC 62325-351 and the IEC 62325-451 series.

A MADES network acts as a post-office organization. The transported object is a “message” in which the sender document is securely repackaged in an envelope (i.e. a header) containing all the necessary information for tracking, transportation and delivery.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*

IETF RFC 1738, *Uniform resource locators (URL)*, <http://www.ietf.org/rfc/rfc1738.txt>

IETF RFC 3110, *RSA/SHA-1 SIGs and RSA KEYs in the domain name system (DNS)*, <http://www.ietf.org/rfc/rfc3110.txt>

IETF RFC 4122, *A universally unique identifier (UUID) URN namespace*, <http://www.ietf.org/rfc/rfc4122.txt>

ITU-T Recommendation X.509, *Information technology - Open systems interconnection - The directory: Public-key and attribute certificate frameworks*, <http://www.itu.int/rec/T-REC-X.509/en>

Withdrawn