

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Cadre pour les communications pour le marché de l'énergie –
Partie 503: Lignes directrices concernant les échanges de données du marché
pour le profil défini dans l'IEC 62325-351**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-5916-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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 the purpose of MADES?	12
4.2 Overview.....	13
4.3 Transparent and reliable message delivery	14
4.4 Components of a MADES system.....	15
4.4.1 Endpoint, broker and component-directory.....	15
4.4.2 Delivery routes and acknowledgements	16
4.4.3 Sharing configuration data of the system	17
4.4.4 Interfaces exposed by the components	19
4.4.5 Architecture examples of MADES systems.....	21
4.5 Security and message integrity	24
4.5.1 Security goals and security solution.....	24
4.5.2 Transport-layer security	25
4.5.3 Message-level security: signing and encryption	26
4.5.4 Non-repudiation	27
5 Delivering the messages.....	29
5.1 Unique identification of components and messages	29
5.2 Message-type of a message	29
5.3 Message route towards a recipient endpoint: message-paths.....	29
5.4 Restriction on the routes by a broker	31
5.5 Message acceptance by a sender endpoint.....	31
5.6 Tracking the delivery of a message.....	31
5.6.1 Message-status of a message	31
5.6.2 Delivery events and acknowledgements.....	32
5.7 Message expiration.....	34
5.8 Reliable transfer of a message.....	35
5.8.1 Rationale	35
5.8.2 Transfer between sender application and sender endpoint.....	36
5.8.3 Transfer between components using the AMQP protocol	37
5.8.4 Transfer between recipient endpoint and recipient application	37
5.9 Storing internal messages in components	38
5.10 Message priority	38
5.11 Message delivery order.....	38
5.12 Testing a route between two endpoints: tracing-messages.....	38
6 Transferring messages using the AMQP protocol.....	39
6.1 Main principles of the AMQP specification	39
6.1.1 Introduction	39
6.1.2 Connection Open.....	40
6.1.3 Session begin.....	40
6.1.4 Link attachment.....	41
6.1.5 Message transfer.....	41

6.1.6	Link recovery and resends	41
6.1.7	Error management	41
6.1.8	Message structure	41
6.2	AMQP high-level implementation: the client/broker model	42
6.3	AMQP implementation in MADES components	43
6.4	Management of AMQP connections and attachments by an endpoint	45
6.5	Internal message format	46
6.5.1	Definitions, design and security checks	46
6.5.2	AMQP format for transferring internal messages	46
6.5.3	Encryption	47
6.5.4	Signing	48
6.5.5	Internal message metadata	49
6.5.6	XML signature example	53
7	Managing configuration data of the system	54
7.1	Rationale	54
7.2	Directory content and information ownership	54
7.3	On the consistency of configuration data	56
7.3.1	Component consistency	56
7.3.2	System consistency	57
7.3.3	Distributed update implementation	57
7.3.4	Eventual consistency	57
7.4	Connection to a component-directory	57
7.5	REST API implementation and available resources	58
7.6	Registration process	59
7.7	Synchronisation process	60
7.7.1	Validity period of replicated data: time-to-live	60
7.7.2	Limitation of the synchronisation flow	60
7.7.3	Configuration of the synchronisation process	61
7.8	XML schemas of the APIs requests and responses	61
7.8.1	Shared types	61
7.8.2	registrations resource	63
7.8.3	endpoints, brokers and components resources	65
8	Managing the certificates	66
8.1	Definitions and principles	66
8.2	Certificates: format and unique ID	67
8.3	Used certificates and issuers certificates authorities	67
8.3.1	Overview	67
8.3.2	Transport-layer security (authorise data exchanges)	67
8.3.3	Message-level security (protect message confidentiality and authenticate message issuer)	68
8.4	Trusting the certificates of others components	68
8.4.1	Authentication	68
8.4.2	Signing and encryption	68
8.5	Renewing the (nearly) expired certificates	68
8.6	Revoking a component	69
9	Managing the version of the MADES specification	69
9.1	MADES version of this document	69
9.2	Issue, version meaning, upgrading recommendations	69
9.3	Changing the signature or the encryption algorithms	70

10	Administrating and operating the components.....	70
11	Interfaces for the applications.....	71
11.1	Endpoint webservice interface for applications.....	71
11.1.1	Overview	71
11.1.2	SendMessage service.....	72
11.1.3	ReceiveMessage service	73
11.1.4	ConfirmReceiveMessage service	75
11.1.5	CheckMessageStatus service	75
11.1.6	ConnectivityTest service.....	77
11.1.7	WSDL for the endpoint webservice interface.....	77
11.2	File System Shared Folders (FSSF).....	84
11.2.1	Overview	84
11.2.2	Folders and file naming convention.....	84
11.2.3	Concurrent access to files	86
11.2.4	Configuring FSSF	86
	Bibliography.....	87
	Figure 1 – MADES overall view.....	12
	Figure 2 – MADES scope in a layered architecture	13
	Figure 3 – MADES message delivery	14
	Figure 4 – MADES components, interactions and protocols	15
	Figure 5 – Possible routes for delivering a message	16
	Figure 6 – Communication protocols for delivering a message	17
	Figure 7 – Data flows between a component-directory and its registered components.....	18
	Figure 8 – Data flows with several component-directories	19
	Figure 9 – Component-directory services and protocols	19
	Figure 10 – MADES Interfaces, services and protocols.....	20
	Figure 11 – Minimal MADES system (without broker).....	21
	Figure 12 – Minimal MADES system (with broker).....	21
	Figure 13 – MADES system with a party in a central role	22
	Figure 14 – MADES system with several brokers	23
	Figure 15 – Using a single endpoint for several business processes	24
	Figure 16 – MADES transport security	25
	Figure 17 – Security: protected endpoint.....	25
	Figure 18 – Security: exposed endpoint	26
	Figure 19 – Message signing and signature verification	26
	Figure 20 – Message encryption and decryption	27
	Figure 21 – Non-repudiation	28
	Figure 22 – Message-status along the delivery	32
	Figure 23 – Tracking events while delivering a message.....	33
	Figure 24 – Reliable transfer.....	36
	Figure 25 –Transfer between sender application and sender endpoint	36
	Figure 26 – Transfer between recipient endpoint and recipient application.....	37
	Figure 27 – The nine AMQP frames	40
	Figure 28 – Structure of an AMQP message	42

Figure 29 – AMQP in MADES components.....	44
Figure 30 – Certificates and certification authorities (CAs) of a MADES system	67
Figure 31 – WSDL 1.1 definitions.....	78
Table 1 – Characteristics of the tracking events.....	34
Table 2 – Final state of a message in an endpoint	38
Table 3 – Services of the client / broker model.....	43
Table 4 – Rules for setting up connection/attachment and for message transfer	45
Table 5 – Internal message – AMQP format: header section	46
Table 6 – Internal message – AMQP format: properties section	46
Table 7 – Internal message – AMQP format: application-properties section	47
Table 8 – Internal message – AMQP format: application-data section	47
Table 9 – Encryption – Processing metadata attributes for the "AES-256" cipher	48
Table 10 – Signing – Processing metadata attributes for the "SHA-512" Algorithm.....	49
Table 11 – MessageMetadata (type).....	50
Table 12 – InternalMessageType (type: string enumeration)	51
Table 13 – ProcessingMetadata (type).....	51
Table 14 – MessageProcessor (type).....	51
Table 15 – Map (type).....	51
Table 16 – MapEntry (type).....	51
Table 17 – ValueType (type: string enumeration).....	52
Table 18 – Component-directory – content of an entry	55
Table 19 – Certificate (type).....	55
Table 20 – MakesImplementation (type)	56
Table 21 – MessagePath (type)	56
Table 22 – BrokerRestriction (type).....	56
Table 23 – HTTP operations	58
Table 24 – HTTP return codes	58
Table 25 – Component-directory API	59
Table 26 – Endpoint interface – Generic error.....	72
Table 27 – Endpoint interface – Value for errorCode.....	72
Table 28 – SendMessage – Request elements.....	72
Table 29 – SentMessage (type)	73
Table 30 – SendMessage – Response elements	73
Table 31 – SendMessage – Additional error elements.....	73
Table 32 – ReceiveMessage – Request elements	74
Table 33 – ReceiveMessage – Response elements.....	74
Table 34 – ReceivedMessage (type)	74
Table 35 – ReceiveMessage – Additional error elements	74
Table 36 – ConfirmReceiveMessage – Request elements	75
Table 37 – ConfirmReceiveMessage – Response elements	75
Table 38 – ConfirmReceiveMessage – Additional error elements	75
Table 39 – CheckMessageStatus – Request elements	75

Table 40 – CheckMessageStatus – Response elements	76
Table 41 – MessageStatus (type).....	76
Table 42 – MessageTraceItem (type).....	76
Table 43 – MessageState or MessageTraceState (Type: string enumeration)	76
Table 44 – CheckMessageStatus – Additional error elements	77
Table 45 – ConnectivityTest – Request elements	77
Table 46 – ConnectivityTest – Response elements	77
Table 47 – ConnectivityTest – Additional error elements	77
Table 48 – FSSF – Folders and filename format	85
Table 49 – FSSF – Tokens used to generate the filenames.....	85

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.

International Standard IEC 62325-503 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This edition cancels and replaces IEC TS 62325-503 published in 2014.

This edition includes the following significant technical changes with respect to the previous edition:

- a) Use of ISO/IEC 19464:2014, Advanced Message Queuing Protocol (AMQP) v1.0 specification;
- b) Splitting of the node described in the IEC TS 62325-503:2014 into a broker that implements the messaging function and a directory;
- c) Increase of operability and resilience of the communication system with the ability for an endpoint to send and receive messages through several brokers;
- d) Benefits of standardisation, performance and scalability of the AMQP protocol for transferring messages.

The text of this standard is based on the following documents:

CDV	Report on voting
57/1936/CDV	57/1983/RVC

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

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

In this document, the following print types are used:

Help the visibility of information in table and diagram: in italic type

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 document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

INTRODUCTION

This document is part of the IEC 62325 series for deregulated energy market communications.

The principal objective of the IEC 62325 series is to produce documents 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 documents specify the content of the messages exchanged.

The purpose of this document 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, harmonised, 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 document 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 document 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 part of IEC 62325 is for European electricity markets.

This document specifies a standard for a communication platform which every Transmission System Operator (TSO) in Europe can use to exchange reliably and securely documents for the energy market. Consequently a European market participant (TSO, regional supervision centre, distribution utility, power exchange, etc.) could benefit from a single, common, harmonised and secure platform for message exchange with other participants; thus, reducing the cost of building different information technology (IT) platforms to interface with all the parties involved.

“MADES” (Market Data Exchange Standard) is the acronym to designate this standard.

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

- From an application program perspective, MADES specifies the software interfaces to exchange electronic documents with peer applications. Such interfaces mainly provide means to send and receive documents using a so-called “MADES communication system” (or “MADES system” or simply “system”). The sender can request about the status of the delivery of a document and the recipient issues a message back, the acknowledgement, when receiving the document. This makes a MADES system usable for exchanging documents in business processes requiring a reliable delivery.
- MADES also specifies services hidden to the applications such as recipient localisation, recipient connection status, message routing and security. Services include directory, authentication, signing, encryption, message tracking, message logging and message temporary storage.

The purpose of MADES is to create a secured message exchange standard based on standard communication protocols and utilising IT best practices for exchanging data over any TCP/IP communication network, in order to facilitate business-to-business (B2B) information exchanges as described in IEC 62325-351 and the IEC 62325-451 series.

A MADES system acts as a post-office organisation: the transported object is a “message” in which the document of the sender is securely packaged in an envelope containing metadata, which is necessary information for transportation, tracking and delivery.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 19464:2014, *Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification*, <https://www.amqp.org/> (developed by the OASIS open standards consortium)

ISO/IEC 9594-8:2017, *Information technology – Open systems interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

SOMMAIRE

AVANT-PROPOS	93
INTRODUCTION.....	95
1 Domaine d'application	96
2 Références normatives	96
3 Termes et définitions	97
4 Concepts évolués	98
4.1 À quoi sert MADES ?	98
4.2 Présentation	100
4.3 Livraison fiable et transparente de messages	100
4.4 Composants d'un système MADES	102
4.4.1 Point d'extrémité, courtier et annuaire des composants (component-directory)	102
4.4.2 Parcours de livraison et accusés de réception	103
4.4.3 Partage des données de configuration du système	104
4.4.4 Interfaces exposées par les composants	106
4.4.5 Exemples d'architecture des systèmes MADES	108
4.5 Sécurité et intégrité des messages	111
4.5.1 Objectifs et solution de sécurité	111
4.5.2 Sécurité de la couche transport	112
4.5.3 Sécurité au niveau du message: signature et chiffrement	113
4.5.4 Non-répudiation	115
5 Livraison des messages	116
5.1 Identification unique des composants et des messages	116
5.2 Attribut «type de message» (message-type) d'un message	116
5.3 Parcours d'un message vers le point d'extrémité d'un destinataire: chemins de message	117
5.4 Restriction des parcours par un courtier	118
5.5 Acceptation d'un message par un point d'extrémité expéditeur	119
5.6 Suivi de la livraison d'un message	119
5.6.1 Attribut «état du message» (message-status) d'un message.....	119
5.6.2 Événements de livraison et accusés de réception	120
5.7 Expiration d'un message	121
5.8 Transfert fiable d'un message	122
5.8.1 Justifications	122
5.8.2 Transfert entre une application expéditrice et un point d'extrémité expéditeur	123
5.8.3 Transfert entre les composants utilisant le protocole AMQP	124
5.8.4 Transfert entre le point d'extrémité destinataire et l'application destinatrice.....	124
5.9 Archivage des messages internes dans les composants	125
5.10 Priorité des messages.....	126
5.11 Ordre de livraison des messages	126
5.12 Vérification par essai d'un parcours entre deux points d'extrémité: messages de traçage (<i>tracing-messages</i>).....	126
6 Transfert de messages via le protocole AMQP	127
6.1 Principes essentiels de la spécification AMQP	127
6.1.1 Introduction	127

6.1.2	Ouvrir une connexion.....	128
6.1.3	Démarrer une session.....	128
6.1.4	Établissement d'une liaison	129
6.1.5	Transfert de messages	129
6.1.6	Reprise de liaisons et nouveaux envois	129
6.1.7	Gestion des erreurs	130
6.1.8	Structure du message.....	130
6.2	Mise en œuvre évoluée du protocole AMQP: modèle client/courtier	130
6.3	Mise en œuvre du protocole AMQP dans les composants MADES	131
6.4	Gestion des connexions et des établissements de liaisons AMQP par un point d'extrémité	133
6.5	Format de message interne.....	134
6.5.1	Définitions, conception et vérifications de sécurité.....	134
6.5.2	Format AMQP de transfert des messages internes	134
6.5.3	Chiffrement.....	135
6.5.4	Signature.....	136
6.5.5	Métadonnées de message interne	138
6.5.6	Exemple de signature XML	141
7	Gestion des données de configuration du système	142
7.1	Justifications.....	142
7.2	Contenu d'un annuaire et détention des informations	142
7.3	Informations concernant la cohérence des données de configuration	145
7.3.1	Cohérence des composants.....	145
7.3.2	Cohérence du système	145
7.3.3	Mise en œuvre de la mise à jour répartie	145
7.3.4	Cohérence finale	146
7.4	Connexion à un annuaire des composants	146
7.5	Mise en œuvre API REST et ressources disponibles	146
7.6	Processus d'enregistrement.....	148
7.7	Processus de synchronisation.....	149
7.7.1	Période de validité des données répliquées: durée de vie (time-to-live ou TTL).....	149
7.7.2	Limitation du flux de synchronisation	149
7.7.3	Configuration du processus de synchronisation	150
7.8	Schémas XML des demandes et réponses des API.....	150
7.8.1	Types partagés.....	150
7.8.2	Ressources pour enregistrements.....	153
7.8.3	Ressources pour points d'extrémité, courtiers et composants	154
8	Gestion des certificats	155
8.1	Définitions et principes.....	155
8.2	Certificats: format et identifiant unique	156
8.3	Certificats utilisés et autorités de délivrance (certificats, autorités)	157
8.3.1	Présentation	157
8.3.2	Sécurité de la couche transport (autorise les échanges de données).....	157
8.3.3	Sécurité au niveau du message (protection de la confidentialité du message et authentification de l'émetteur du message).....	158
8.4	Fiabilité des certificats d'autres composants	158
8.4.1	Authentification.....	158
8.4.2	Signature et chiffrement.....	158

8.5	Renouvellement des certificats (quasi) expirés	158
8.6	Révocation d'un composant	159
9	Gestion de la version de la spécification MADES	159
9.1	Version MADES du présent document.....	159
9.2	Objectif et signification de la version, recommandations pour les mises à niveau.....	159
9.3	Modification des algorithmes de signature ou de chiffrement.....	160
10	Administration et exploitation des composants.....	161
11	Interfaces pour les applications	161
11.1	Interface des services Web des points d'extrémité pour les applications	161
11.1.1	Présentation	161
11.1.2	Service SendMessage	162
11.1.3	Service ReceiveMessage.....	164
11.1.4	Service ConfirmReceiveMessage.....	165
11.1.5	Service CheckMessageStatus.....	166
11.1.6	Service ConnectivityTest	168
11.1.7	Langage WSDL pour l'interface des services Web des points d'extrémité.....	168
11.2	Dossiers partagés d'un système de fichiers (FSSF – <i>File System Shared Folders</i>)	175
11.2.1	Présentation	175
11.2.2	Dossiers et convention de nommage des fichiers.....	175
11.2.3	Accès simultané aux fichiers.....	177
11.2.4	Configuration de FSSF	177
	Bibliographie.....	179
	Figure 1 – Aperçu général de MADES.....	98
	Figure 2 – Domaine d'application de MADES dans une architecture en couches.....	100
	Figure 3 – Livraison de messages MADES.....	101
	Figure 4 – Composants, interactions et protocoles d'un système MADES	102
	Figure 5 – Parcours possibles pour la livraison d'un message.....	103
	Figure 6 – Protocoles de communication pour la livraison d'un message	104
	Figure 7 – Flux de données entre un annuaire des composants et ses composants enregistrés.....	105
	Figure 8 – Flux de données avec plusieurs annuaires des composants.....	106
	Figure 9 – Services et protocoles d'un annuaire des composants	106
	Figure 10 – Interfaces, services et protocoles MADES	107
	Figure 11 – Système MADES minimal (sans courtier)	108
	Figure 12 – Système MADES minimal (avec courtier)	109
	Figure 13 – Système MADES avec une partie dont le rôle est central	109
	Figure 14 – Système MADES avec plusieurs courtiers	110
	Figure 15 – Utilisation d'un seul point d'extrémité pour plusieurs processus métiers	111
	Figure 16 – Sécurité de transport MADES.....	112
	Figure 17 – Sécurité: point d'extrémité protégé.....	113
	Figure 18 – Sécurité: point d'extrémité exposé.....	113
	Figure 19 – Signature de message et vérification de la signature.....	114

Figure 20 – Chiffrement et déchiffrement de message	114
Figure 21 – Non-répudiation	115
Figure 22 – État du message tout au long du processus de livraison.....	119
Figure 23 – Événements de suivi lors de la livraison d'un message	120
Figure 24 – Transfert fiable.....	123
Figure 25 – Transfert entre l'application expéditrice et le point d'extrémité expéditeur	124
Figure 26 – Transfert entre le point d'extrémité destinataire et l'application destinatrice	125
Figure 27 – Les neuf trames AMQP	128
Figure 28 – Structure d'un message AMQP.....	130
Figure 29 – Protocole AMQP dans les composants MADES	132
Figure 30 – Certificats et autorités de certification (CA) d'un système MADES.....	157
Figure 31 – Définitions WSDL 1.1	169
Tableau 1 – Caractéristiques des événements de suivi	121
Tableau 2 – État final d'un message dans un point d'extrémité	126
Tableau 3 – Services du modèle client / courtier	131
Tableau 4 – Règles de mise en place d'une connexion/d'un établissement de liaison et règles de transfert de messages	133
Tableau 5 – Message interne – Format AMQP: section Header.....	135
Tableau 6 – Message interne – Format AMQP: section Properties	135
Tableau 7 – Message interne – Format AMQP: section Application-properties	135
Tableau 8 – Message interne – Format AMQP: section Application-data.....	135
Tableau 9 – Chiffrement – Attributs de métadonnées de traitement pour le chiffre 'AES-256'	136
Tableau 10 – Signature – Attributs de métadonnées de traitement pour l'algorithme 'SHA-512'	137
Tableau 11 – Métadonnées de message (type)	138
Tableau 12 – InternalMessageType (type: énumération de chaînes)	139
Tableau 13 – ProcessingMetadata (type)	139
Tableau 14 – MessageProcessor (type)	139
Tableau 15 – Map (type)	139
Tableau 16 – MapEntry (type).....	139
Tableau 17 – ValueType (type: énumération de chaînes).....	140
Tableau 18 – Annuaire des composants – contenu d'une entrée	143
Tableau 19 – Certificat (type).....	144
Tableau 20 – MadesImplementation (type).....	144
Tableau 21 – MessagePath (type).....	144
Tableau 22 – BrokerRestriction (type).....	144
Tableau 23 – Opérations HTTP.....	146
Tableau 24 – Codes de retour HTTP.....	147
Tableau 25 – API d'annuaire des composants.....	148
Tableau 26 – Interface des points d'extrémité – Erreur générique	162
Tableau 27 – Interface des points d'extrémité – Valeur pour errorCode	162
Tableau 28 – SendMessage – Éléments de la demande	163

Tableau 29 – SentMessage (type).....	163
Tableau 30 – SendMessage – Éléments de la réponse	163
Tableau 31 – SendMessage – Éléments d’erreur supplémentaires.....	164
Tableau 32 – ReceiveMessage – Éléments de la demande	164
Tableau 33 – ReceiveMessage – Éléments de la réponse.....	164
Tableau 34 – ReceivedMessage (type)	165
Tableau 35 – ReceiveMessage – Éléments d’erreur supplémentaires	165
Tableau 36 – ConfirmReceiveMessage – Éléments de la demande	166
Tableau 37 – ConfirmReceiveMessage – Éléments de la réponse.....	166
Tableau 38 – ConfirmReceiveMessage – Éléments d’erreur supplémentaires	166
Tableau 39 – CheckMessageStatus – Éléments de la demande	166
Tableau 40 – CheckMessageStatus – Éléments de la réponse.....	166
Tableau 41 – MessageStatus (type).....	167
Tableau 42 – MessageTraceItem (type)	167
Tableau 43 – MessageState ou MessageTraceState (Type: énumération de chaîne)	167
Tableau 44 – CheckMessageStatus – Éléments d’erreur supplémentaires	168
Tableau 45 – ConnectivityTest – Éléments de la demande.....	168
Tableau 46 – ConnectivityTest – Éléments de la réponse	168
Tableau 47 – ConnectivityTest – Éléments d’erreur supplémentaires	168
Tableau 48 – FSSF – Dossiers et format de nom de fichier.....	176
Tableau 49 – FSSF – Jetons utilisés pour générer les noms de fichiers	177

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**CADRE POUR LES COMMUNICATIONS
POUR LE MARCHÉ DE L'ÉNERGIE –****Partie 503: Lignes directrices concernant les échanges
de données du marché pour le profil défini dans l'IEC 62325-351**

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62325-503 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Cette édition annule et remplace l'IEC TS 62325-503 parue en 2014.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- a) Utilisation de l'ISO/IEC 19464:2014, Advanced Message Queuing Protocol (AMQP) v1.0 specification (disponible en anglais seulement);
- b) Répartition du nœud décrit dans l'IEC TS 62325-503:2014 dans un courtier qui met en œuvre la fonction de transmission de messages et un annuaire;

- c) Renforcement de l'opérabilité et de la résilience du système de communication avec capacité pour un point d'extrémité d'envoyer et de recevoir des messages par l'intermédiaire de plusieurs courtiers;
- d) Avantage issu de la normalisation, des performances et de l'évolutivité du protocole AMQP de transfert de messages.

Le texte de cette norme est issu des documents suivants:

CDV	Rapport de vote
57/1936/CDV	57/1983/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Dans ce document, les caractères suivants sont utilisés:

Facilitation de la visibilité de l'information dans les tableaux et diagrammes: en italique

Une liste de toutes les parties de la série IEC 62325, publiées sous le titre général *Cadre pour les communications pour le marché de l'énergie* peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le présent document fait partie de la série IEC 62325 concernant les communications relatives au marché déréglementé de l'énergie.

Le principal objectif de la série de normes IEC 62325 est de produire des documents destinés à faciliter l'intégration de logiciels d'application pour le marché, développés de façon indépendante par différents fournisseurs, dans un système de gestion de marché et entre des systèmes de gestion de marché et des systèmes participant au marché. Pour ce faire, des échanges de messages sont définis afin de permettre à ces applications ou systèmes d'accéder aux données publiques et d'échanger des informations, indépendamment de la façon dont ces informations sont représentées en interne.

Le modèle d'information commun (CIM, *common information model*), spécifie la base d'une sémantique d'échange des messages. Les spécifications d'un profil marché de style européen qui couvrent les besoins des marchés de l'électricité conçus selon le style européen sont définies dans l'IEC 62325-351. Ces marchés de l'électricité respectent la réglementation européenne et appliquent les concepts d'accès tiers et de découpage des marchés en zones. Les normes internationales IEC 62325-451-n spécifient le contenu des messages échangés.

L'objet du présent document est de fournir des lignes directrices dédiées à l'échange des messages susmentionnés. Un participant aux marchés européens (opérateur, régies de distribution, etc.) peut tirer profit d'une plate-forme commune harmonisée et sûre d'échange des messages avec les gestionnaires de réseaux de transport (GRT), réduisant ainsi le coût de mise en place de différentes plates-formes TI assurant l'interface avec toutes les parties concernées.

Le présent document représente une étape importante permettant aux parties de participer à des marchés de l'électricité autres que leurs marchés nationaux. Elles peuvent utiliser le même système d'échange d'informations ou un système analogue pour participer à deux marchés ou plus dans toute l'Europe.

À l'origine, le présent document s'appuyait sur les travaux du groupe de travail EDI du Réseau européen des gestionnaires de réseaux de transport d'électricité (ENTSO-E – *European Network of Transmission System Operators*).

CADRE POUR LES COMMUNICATIONS POUR LE MARCHÉ DE L'ÉNERGIE –

Partie 503: Lignes directrices concernant les échanges de données du marché pour le profil défini dans l'IEC 62325-351

1 Domaine d'application

La présente partie de l'IEC 62325 est destinée aux marchés européens de l'électricité.

Le présent document spécifie une norme relative à une plate-forme de communication que chaque gestionnaire de réseau de transport (GRT) en Europe peut utiliser pour échanger en toute fiabilité et sécurité des documents destinés au marché de l'énergie. Par conséquent, un participant aux marchés européens (GRT, centre régional de surveillance, régie de distribution, bourse d'électricité, etc.) peut tirer profit d'une plate-forme commune unique harmonisée et sûre d'échange des messages avec les autres participants, réduisant ainsi le coût de mise en place de différentes plates-formes de technologies de l'information (TI) assurant l'interface avec toutes les parties concernées.

MADES (Norme d'échange de données marché ou *MArket Data Exchange Standard* en anglais) est l'acronyme qui désigne la présente norme.

MADES constitue une spécification d'une plate-forme de communication commune décentralisée basée sur les normes TI internationales:

- Du point de vue d'une application, MADES spécifie les interfaces logicielles d'échange de documents électroniques avec des applications homologues. Ces interfaces permettent principalement d'envoyer et de recevoir des documents avec un système de communication appelé MADES (ou «système MADES», voire simplement «système»). L'expéditeur peut s'enquérir de l'état de livraison d'un document et le destinataire émet un message en retour, à savoir un accusé de réception, à réception du document. Cette situation permet d'utiliser un système MADES pour échanger des documents dans des processus métiers exigeant une livraison fiable.
- MADES spécifie également les services non perceptibles par les applications tels que la localisation du destinataire, l'état de connexion du destinataire, l'acheminement des messages et la sécurité. Les services comprennent l'annuaire, l'authentification, la signature, le chiffrement, le suivi, la trace et l'archivage temporaire des messages.

MADES a pour objet de produire une norme d'échange sécurisé de messages basée sur des protocoles de communication normalisés et d'appliquer les meilleures pratiques TI pour échanger des données sur tout réseau de communication TCP/IP afin de faciliter les échanges d'informations de métier à métier (B2B) tels que décrits dans les séries IEC 62325-351 et IEC 62325-451.

Un système MADES fonctionne comme une organisation postale: l'objet transporté est un «message» dans lequel le document de l'expéditeur est incorporé en toute sécurité dans une enveloppe contenant des métadonnées qui constituent des informations nécessaires pour le transport, le suivi et la livraison.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée

s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

ISO/IEC 19464:2014 *Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification*, <https://www.amqp.org/> (développé par l'OASIS open standards consortium) (disponible en anglais seulement)

ISO/IEC 9594-8:2017, *Information technology – Open systems interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks* (disponible en anglais seulement)