DIN EN IEC 62325-503

DIN

ICS 27.010; 35.240.50 Einsprüche bis 2019-12-11

Entwurf

Kommunikation im Energiemarkt – Teil 503: Richtlinien zum Austausch von Marktdaten für das Profil der IEC 62325-351 (IEC 62325-503:2018); Englische Fassung EN IEC 62325-503:2018

Framework for energy market communications –
Part 503: Market data exchanges guidelines for the IEC 62325-351 profile
(IEC 62325-503:2018);
English version EN IEC 62325-503:2018

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
(IEC 62325-503:2018);
Version anglaise EN IEC 62325-503:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-11 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 92 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

AVA Documents Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

Nationales Vorwort

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 57 „Power systems management and associated information exchange“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „http://webstore.iec.ch“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument
– bestätigt,
– zurückgezogen,
– durch eine Folgeausgabe ersetzt oder
– geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für den vorliegenden Norm-Entwurf erfüllt.

Da sich die Benutzer des vorliegenden Norm-Entwurfs der englischen Sprache als Fachsprache bedienen, wird der englische Text/die Englische Fassung der EN IEC 60325-503:2018 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Norm-Entwurfs hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Norm-Entwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

Nationaler Anhang NA
(informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

1 Anwendungsbereich

Dieser Teil der IEC 62325 ist für die europäischen Strommärkte bestimmt.

Dieses Dokument spezifiziert einen Standard für eine Kommunikationsplattform, mit dem jeder Übertragungsnetzbetreiber (TSO) in Europa zuverlässig und sicher Dokumente austauschen kann für den Energiemarkt. Folglich ist ein europäischer Marktteilnehmer (TSO, regionale Aufsicht) Zentrum, Verteilungsnetz, Strombörse, usw.) könnte von einer einzigen, gemeinsamen, harmonisierten und sicheren Plattform für den Nachrichtenaustausch mit anderen Teilnehmern profitieren; also, die Reduzierung die Kosten für den Aufbau verschiedener Informationstechnologie-(IT)-Plattformen, die mit allen Systemen verbunden sind. beteiligte Parteien.

„MADES“ (en: Market Data Exchange Standard) ist das Akronym für die Bezeichnung dieser Norm. MADES ist eine Spezifikation für eine dezentrale gemeinsame Kommunikationsplattform auf Basis von internationale IT-Standards:

- Aus Sicht des Anwendungsprogramms spezifiziert MADES die Softwareschnittstellen zu den folgenden Komponenten Austausch elektronischer Dokumente mit Peer-Anwendungen. Solche Schnittstellen bieten vor allem Mittel zum Senden und Empfangen von Dokumenten über ein sogenanntes „MADES-Kommunikationssystem“. (oder „MADES-System“ oder einfach „System“). Der Absender kann nach dem Status des Zustellung eines Dokuments und der Empfänger gibt eine Nachricht zurück, die Bestätigung, beim Empfang des Dokuments. Dies macht ein MADES-System verwendbar für den Austausch von Dokumente in Geschäftsprozessen, die eine zuverlässige Lieferung erfordern.
- MADES spezifiziert auch Dienste, die für die Anwendungen versteckt sind, wie z. B. die Empfänger-lokalisierung, Empfängerverbindungsstatus, Nachrichtenweiterleitung und Sicherheit. Die Dienste beinhalten ein Verzeichnis, Authentifizierung, Signierung, Verschlüsselung, Nachrichtenverfolgung, Nachrichtenprotokollierung und Nachricht Zwischenlagerung.

Der Zweck von MADES ist es, einen sicheren Nachrichtenaustauschstandard zu schaffen, der auf folgenden Elementen basiert Standardkommunikationsprotokolle und die Nutzung von IT-Best-Practice-Verfahren für den Datenaustausch über beliebige Kanäle hinweg. TCP/IP-Kommunikationsnetzwerk, um Business-to-Business (B2B)-Informationen zu ermöglichen. wie in IEC 62325-351 und der Normenreihe IEC 62325-451 beschrieben.

Ein MADES-System fungiert als Postorganisation: Das transportierte Objekt ist eine „Nachricht“ in der die das Dokument des Absenders sicher in einem Umschlag mit Metadaten verpackt ist, die notwendige Informationen für Transport, Verfolgung und Lieferung sind.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC TS 61970-2 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

– IEC Electropedia: verfügbar unter http://www.electropedia.org/
– ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

AVA Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

ANMERKUNG Allgemeine Glossardefinitionen siehe IEC 60050, International Electrotechnical Vocabulary.

3.1
erweitertes Protokoll für die Nachrichtenwarteschlange
AMQP
(en: advanced message queuing protocol)
offenes Internet-Protokoll für Business-Messaging, wie in IEC 19464:2014 beschrieben

3.2
erweitertes Nachrichtenwarteschlangenprotokoll, das mit Sicherheit auf der Transportschicht gesichert ist
AMQPS
(en: advanced message queuing protocol secured with transport layer security)
Kombination des IEC 19464-Business-Messaging-Protokolls mit Transport Layer Security (TLS)

3.3
Marktdatenaustauschstandard
MADES
(en: market data exchange standard)
in diesem Dokument beschriebene Spezifikation für das europäische Marktstil-Marktprofil

3.4
repräsentative Zustandsübertragung
REST
(en: representational state transfer)
Verfahren zur Bereitstellung der Interoperabilität zwischen Computersystemen durch Anforderung des Zugriffs und dem Manipulieren von textlichen Darstellungen von Ressourcen unter Verwendung eines vordefinierten Satzes von zustandslosen Operationen

3.5
einfache Authentifizierungs- und Sicherheitsschicht
SASL
(en: simple authentication and security layer)
Framework für Authentifizierung und Datensicherheit in Internet-Protokollen

3.6
einfaches Objektzugriffsprotokoll
SOAP
(en: simple object access protocol)
Protokollspezifikation zum Austausch strukturierter Informationen bei der Umsetzung von Webservices

3.7
Übertragungsnetzbetreiber
TSO
(en: transmission system operator)
an der Stromübertragung oder dem Transport von Erdgas beteiligte Stelle

3.8
Sicherheit der Transportschicht
TLS
(en: transport layer security)
kryptographisches Protokoll zur Gewährleistung der Privatsphäre und Datenintegrität zwischen zwei kommunizierenden Computeranwendungen

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

EUROPEAN STANDARD — *Entwurf* — **EN IEC 62325-503**

NORME EUROPÉENNE

EUROPÄISCHE NORM

October 2018

ICS 33.200

English Version

Framework for energy market communications - Part 503: Market data exchanges guidelines for the IEC 62325-351 profile (IEC 62325-503:2018)

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
(IEC 62325-503:2018)

Kommunikation im Energiemarkt - Teil 503: Richtlinien zum Austausch von Marktdaten für das Profil der IEC 62325-351
(IEC 62325-503:2018)

This European Standard was approved by CENELEC on 2018-08-30. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

European foreword

The text of document 57/1936/CDV, future edition 1 of IEC 62325-503, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62325-503:2018.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2019-05-30
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-08-30

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62325-503:2018 was approved by CENELEC as a European Standard without any modification.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC TS 61970-2	-	Energy management system application program interface (EMS-API) - Part 2: Glossary	-	-
ISO/IEC 9594-8	2017	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
ISO/IEC 19464:2014	2014	Information technology - Advanced Message Queuing Protocol (AMQP) v1.0 specification	-	-

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

CONTENTS

European foreword 2
Annex ZA (normative) Normative references to international publications with their corresponding European publications 3
CONTENTS 4
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 28
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 30
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

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

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 64
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) 68
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 69

AVA Documents
Document Sharing Hub

8.5 Renewing the (nearly) expired certificates 69
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 70
9.3 Changing the signature or the encryption algorithms 70
10 Administrating and operating the components 71
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 85
11.2.3 Concurrent access to files 86
11.2.4 Configuring FSSF 86
Bibliography 88

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 26
Figure 18 – Security: exposed endpoint 26
Figure 19 – Message signing and signature verification 27
Figure 20 – Message encryption and decryption 27
Figure 21 – Non-repudiation 28

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

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 – MadesImplementation (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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

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 86

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

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.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

— *Entwurf* —

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)

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 61970-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE For general glossary definitions, see IEC 60050, *International Electrotechnical Vocabulary*.

3.1
advanced message queuing protocol
AMQP
open Internet protocol for business messaging, as described in IEC 19464:2014

3.2
advanced message queuing protocol secured with transport layer security
AMQPS
combining of the IEC 19464 business messaging protocol with transport layer security (TLS)

3.3
market data exchange standard
MADES
specification described in this document for the European market style market profile

3.4
representational state transfer
REST
method of providing interoperability between computer systems by requesting to access and manipulate textual representations of resources using predefined set of stateless operations

3.5
simple authentication and security layer
SASL
framework for authentication and data security in internet protocols

3.6
simple object access protocol
SOAP
protocol specification for exchanging structured information in the implementation of webservices

3.7
transmission system operator
TSO
entity involved in electric power transmission or in transmission of natural gas

3.8
transport layer security
TLS
cryptographic protocol to provide privacy and data integrity between two communicating computer applications

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

4 High level concepts

4.1 What is the purpose of MADES?

NOTE Clause 4 describes the business context for the specification usage, introduces the main concepts of the specification and does not contain requirements.

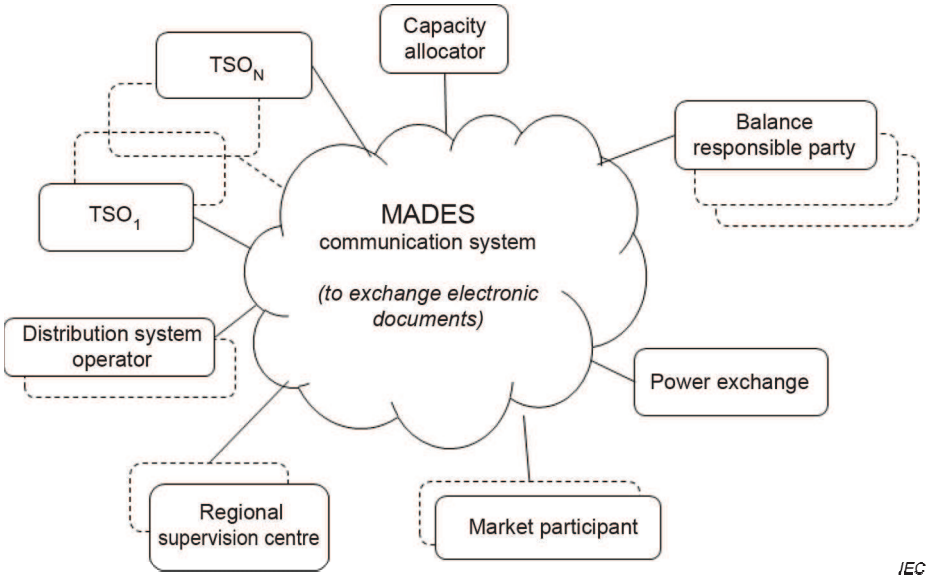

Figure 1 – MADES overall view

MADES' first intention is to provide transmission system operators (TSOs) with a standardised communication system for securely exchanging electronic documents between themselves and with others parties involved in the European electricity market as shown in Figure 1.

These documents are mainly those used in the energy market and described in IEC 62325-351 and the IEC 62325-451 series. Such parties include TSOs, regional supervision centres, power exchanges, distribution system operators, balance responsible parties, transmission capacity allocators, market operators, capacity traders, producers, etc.

MADES enables each party to host an access point to the communication system: applications of his information system can then use the access point to send and receive securely documents with other parties.

Technically, MADES is a data exchange standard comprised of standard communication protocols and utilising information technology standards and best practices to create a mechanism for exchanging data over any TCP/IP communication network and infrastructure, in order to facilitate business-to-business information exchanges.

New market rules induce new business processes and activities, and generally require new information exchanges between parties. Experience shows that, for the data exchanges to meet the business goals, the chosen technical solution results from an agreement of all the involved parties gathering various constraints including implementation time scale, vendors' offers, already existing communication infrastructure and links, integration capabilities of existing information systems, confidentiality of exchanged information, legal risks, performance, etc.

Whereas business processes require that information be exchanged between multiple systems or multiple parties, solutions developed bilaterally can become complex, each interface taking time before coming in operation, taking money and resources for development and maintenance. A noticeable consequence is that some parties involved in business processes that require exchanges

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

with many others parties have to install and operate different communication tools and solutions to interface with multiple information systems. The process towards a more integrated European electricity market creates many such situations with new coordinated processes between actors with regulated roles. Market participants acting in several countries are also looking for a harmonised interface.

MADES can support any business process whatever the transmitted document format (e.g. XML, binary) and the sequence for the exchanges.

MADES is independent of the physical underlying communication Infrastructure, which can be any internet protocol (IP) network, such as Internet, a physical private infrastructure, or a multi access-point virtual private network (VPN).

MADES relies on and only on non-proprietary IT standards for communication protocols, data integrity, peer authentication (signature), confidentiality (encryption), accessible parties' directory (e.g. HTTP, AMQP, TLS, X.509), as shown in Figure 2.

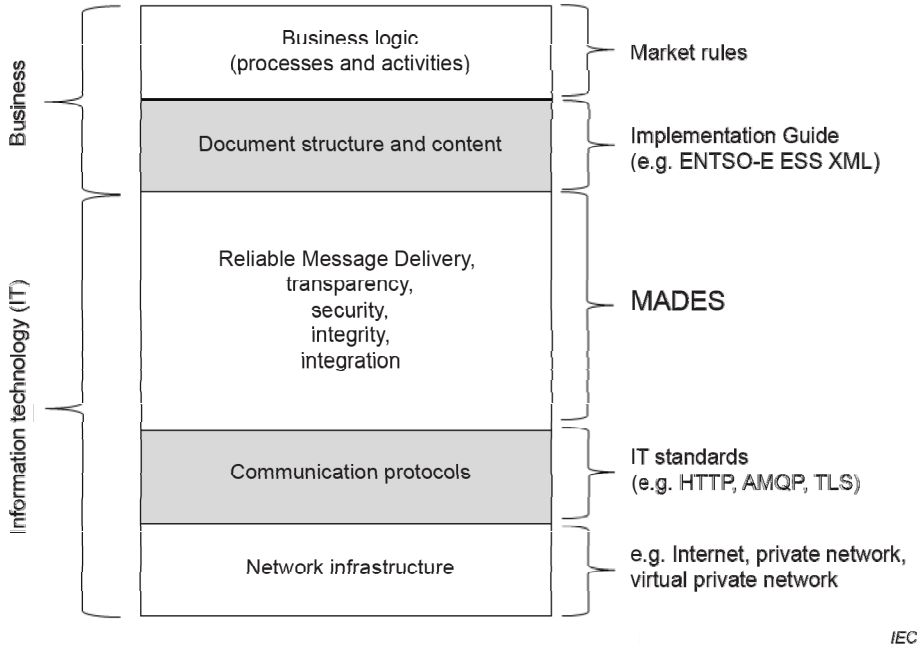

Figure 2 – MADES scope in a layered architecture

4.2 Overview

The MADES standard specifies a communication system that delivers messages between authorised parties. Such a system has the following key features:

1) Reliable message delivery – A (sender) party connected can send a message to another (recipient) party connected or that can connect to the system. The sender is notified when a message is not acknowledged by the recipient in due time, whatever reason.
2) Transparency – The system is not a black box: it tracks every message down to gather trustworthy information about the delivery.
3) Security – Only the recipient of the message can read the content (confidentiality) and the recipient unambiguously authenticates the sender (signature).
4) Integrity – The system guarantees that the content of a message is unaltered during the delivery process.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

5) Integration – A wide variety of technologies can integrate with the services exposed for sending and receiving messages. This eases development and integration in any information system.

The first four key features (reliable message delivery, transparency, security and integrity) are capabilities of the system, while the last one (integration) is a design characteristic of the MADES components.

4.3 Transparent and reliable message delivery

The main feature of a MADES system is the message delivery function, as shown Figure 3.

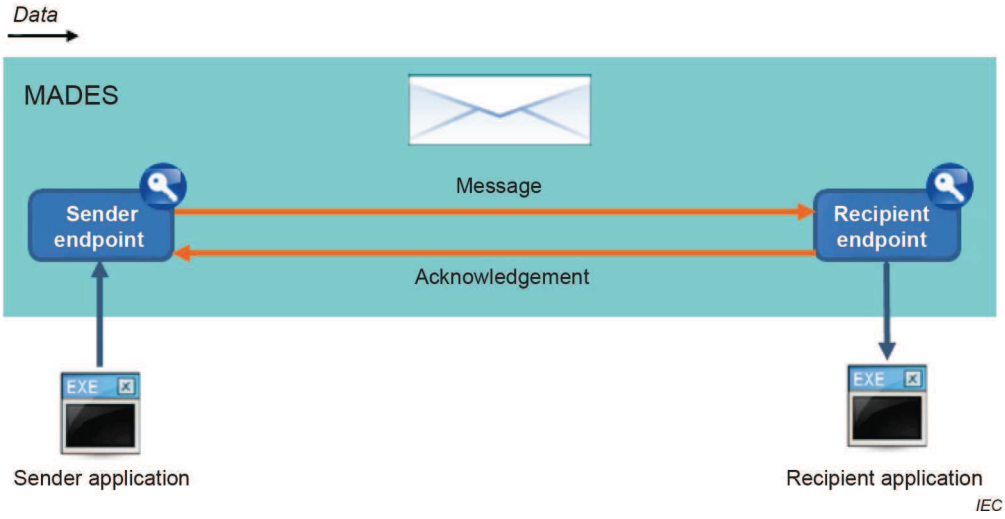

Figure 3 – MADES message delivery

A sender wants or needs to transfer a document to a recipient using the system. Both the sender and the recipient are applications that use an application-programming interface (API) to connect to their respective access points, named *endpoints*.

The peer applications view the system only through the defined interface. The document being transported from one to the other can be any text or binary data. Actually, the system transports a message that comprises the document with additional metadata, which includes information to route and transport the message securely such as a unique ID, the identities of the peer endpoints and cryptographic information related to the message signing and to the document encryption.

The system tracks any message that a sender endpoint accepted. The endpoint can reject a request from a business application for sending a document, e.g. if the recipient is unknown.

The sender application can check at any time the status of a sent message among ACCEPTED, DELIVERED, RECEIVED or FAILED (see 5.6.1).

The sender endpoint knows that the system has delivered a message to the recipient endpoint, when it receives back an acknowledgement issued by the recipient endpoint. The sender endpoint sets the status of the message to FAILED when the message expires, i.e. if it does not receive the acknowledgement in due time, whatever reason.

The system transports both:

- Standard message – a message composed by a sender endpoint to send an electronic document upon request from a sender application.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

- Acknowledgement – a message composed by a recipient endpoint for tracking the endpoint-to-endpoint delivery [1] of a standard message. The applications do not know about acknowledgements, which remain internal to the system.

NOTE Further in the document, the single work "message" refers to "standard message", and "internal message" generically refers to either (standard) message or acknowledgement.

4.4 Components of a MADES system

4.4.1 Endpoint, broker and component-directory

A MADES system is a set of components out of three types: endpoint, broker and component-directory. Two components interact in a client / server mode as shown in Figure 4. This is the full view that the current clause explains in details.

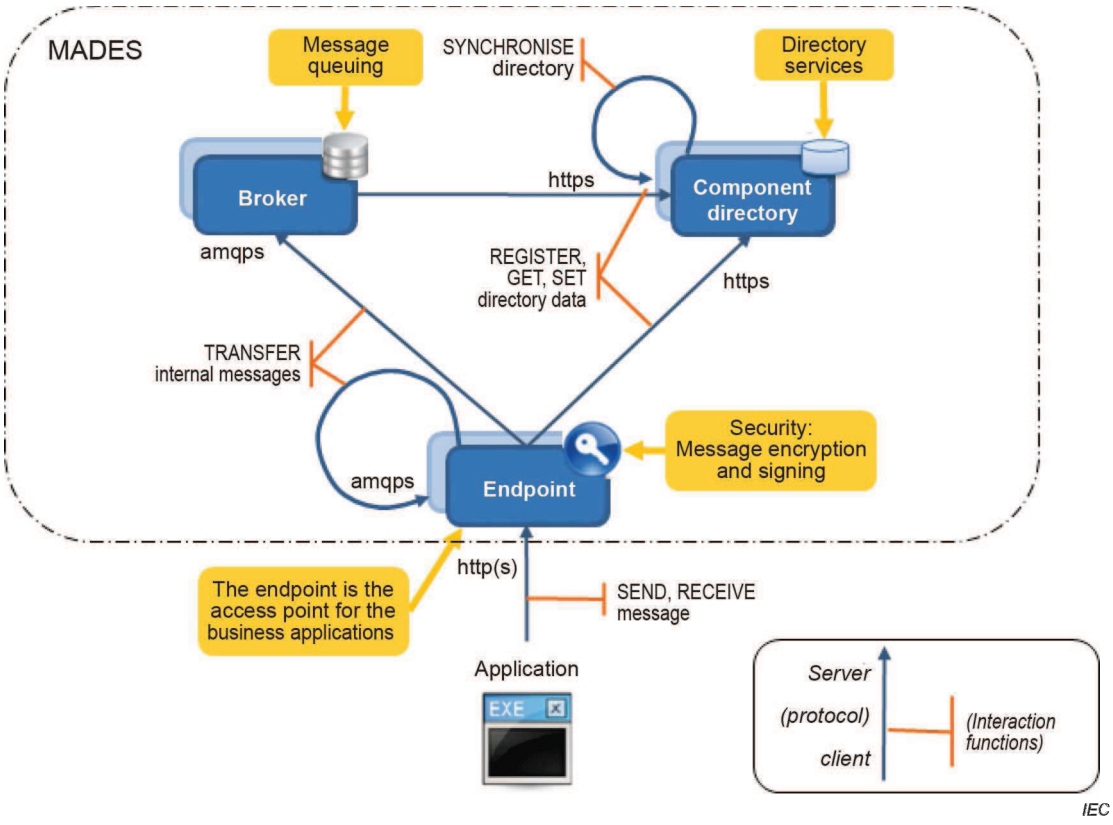

Figure 4 – MADES components, interactions and protocols

A party using the system hosts an endpoint. An application (*client*) uses the interface exposed by the endpoint (*server*) to send and receive messages. The interface uses the HTTP(S) protocol.

NOTE The client component opens a connection. The server component accepts the connection.

This document refers to a sender (respectively recipient) endpoint when focussing on the operations that the endpoint performs for sending (resp. receiving) a message. The endpoints perform the end-to-end security; namely, the sender endpoint signs and encrypts the message, whereas the recipient endpoint decrypts the message and verifies the sender signature.

---

1 This is a technical acknowledgement, not an acknowledgement as defined in IEC 62325-451-1.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

For transferring a message, the sender endpoint (*client*) uploads it to a broker (*server*), and the recipient endpoint *(client)* downloads it from that broker: the broker temporarily stores the message in a queue; this is further referred as an *indirect* transfer. The sender endpoint (*client*) can also upload the message directly to the recipient endpoint (*server*): this is further referred as a *direct* transfer. Whatever route, the protocol to transfer the message is AMQPS, which stands for Advanced Message Queuing Protocol Secured with transport layer security (TLS).

Transferring an acknowledgement works the same way, but the peer endpoints play reverse roles, the recipient being the sender and vice versa. A broker only works with internal messages and does not distinguish between messages and acknowledgements.

The endpoints and the brokers (*all clients*) get configuration data of the system, e.g. identifications of the existing components, certificates, authorised delivery routes, from a component-directory (*a server*), which implements an address book. When the system comprises several component-directories, they synchronise each other. The directory services use the HTTPS protocol.

4.4.2 Delivery routes and acknowledgements

Figure 5 shows the possible routes to transfer a message:

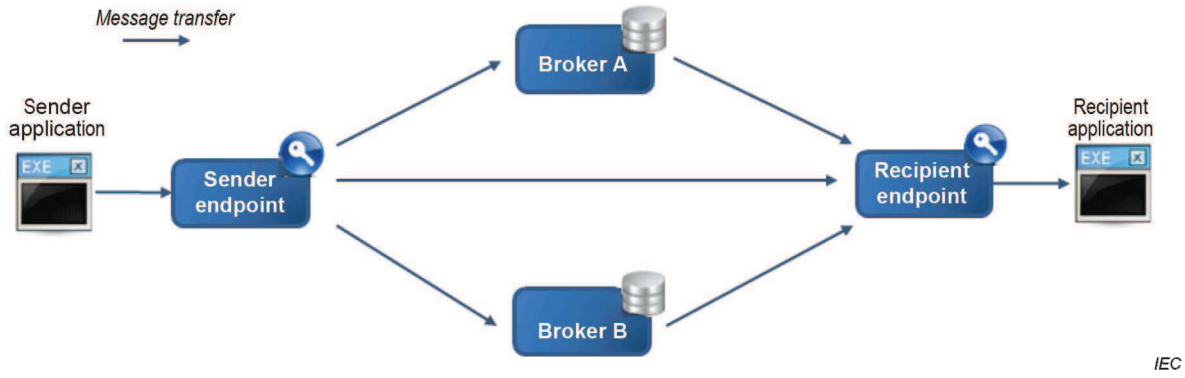

Figure 5 – Possible routes for delivering a message

A sender endpoint can transfer a message to a recipient endpoint either using an intermediate broker or directly. Enabling or not enabling direct transfer is a security issue (see 4.5.2).

Figure 5 shows that the system can include several brokers and that the messages between two given endpoints can use different routes. The route depends on the type of the document to transport, named after the *message-type*, which generally binds the message to some business process (see 5.2). The sender endpoint selects the route according to the message-path (see 5.3) associated with the message-type, as configured by the *recipient* endpoint, and published and accessible in the components-directories.

Figure 6 shows the communication protocols used along the message route.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

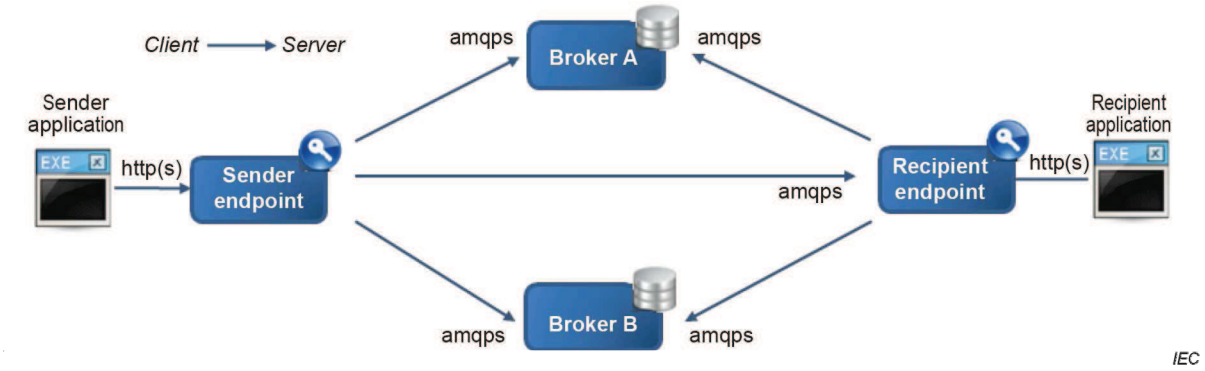

Figure 6 – Communication protocols for delivering a message

An acknowledgement is an internal message issued by the recipient endpoint back to the sender endpoint to notify that it received a message. The route of the acknowledgement is the *exact reverse route* of the corresponding message.

NOTE:

- The sender application sets the message-type but does not select the route. Modifying a message-path changes the route but does not affect the applications.
- Load balancing the message traffic through multiple brokers is not possible. Between two given endpoints, all messages with the same message-type use the same route. Some brokers can support high available clustered setups.
- There is at most one broker on the route from a sender endpoint to a recipient endpoint.

4.4.3 Sharing configuration data of the system

Implementing message routing and security transparently to applications enforces that the endpoints and the brokers access to configuration data that describes the system. This includes the following information for each component:

- unique ID,
- security certificates for authentication, signing and encryption,
- telecommunication network location to access the services that the component exposes,
- rules for message delivery: for an endpoint, the rules say what are the routes to send messages to the endpoint; for a broker the rules say which messages the broker accepts, i.e. which message-types and from which sender endpoints,
- operational contact information.

Each endpoint and each broker registers with a single component-directory, named after its *home component-directory*. A major role of the administrator of a component-directory is to accept new parties, establish trust with them, and to register their components. The role includes the reverse operations: unregister components, notably the ones potentially compromised. A component-directory and the set of its registered components forms a *subsystem*.

Figure 7 shows data flows between a component-directory "A" and its registered components:

(A) When accepting a registration request, the component-directory creates a new entry for the component in the directory. It also issues and stores the component certificates.

(B) The administrator of a registered component enters all of configuration data about the component, which is pushed for update in the home component-directory.

(C) A registered component locally caches the whole directory content and cyclically request for synchronisation. On a change, it receives a full copy of the directory, not increments.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

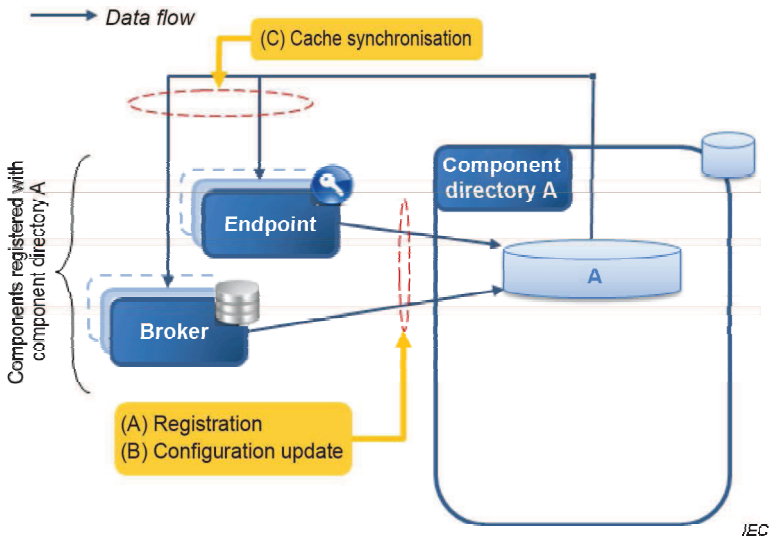

Figure 7 – Data flows between a component-directory and its registered components

The specification of the component-directory pursues two goals:

1) Minimise the administration tasks: data entry is limited. In addition, whereas the first registration should probably always require a manual acceptance, the certificates renewal could [2] be automatic (see 7.6) in case the request comes from a validly registered component.
2) Design a non-critical component, i.e. which does not block the message transfer when it is down. Indeed, each endpoint and each broker locally caches and refreshes directory data, which remains valid during a configurable period while the component-directory is down.

Figure 8 shows the same component-directory "A", now included in a wider system with two other subsystems, i.e. component-directories: "B" and "C".

- every component-directory couple synchronises bi-directionally, i.e. each directory requests the other for its subsystem directory content;
- an "A"-registered endpoint (respectively broker) now receives the entire system directory content ("A" + "B" + "C") when synchronising with its home component-directory;
- a "B"-registered or "C"-registered component synchronises with the "A" component-directory when its home component-directory is down. Conversely an "A"-registered component can synchronise with another component-directory (such a flow is not presented in Figure 8).

2 This is a system governance decision.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

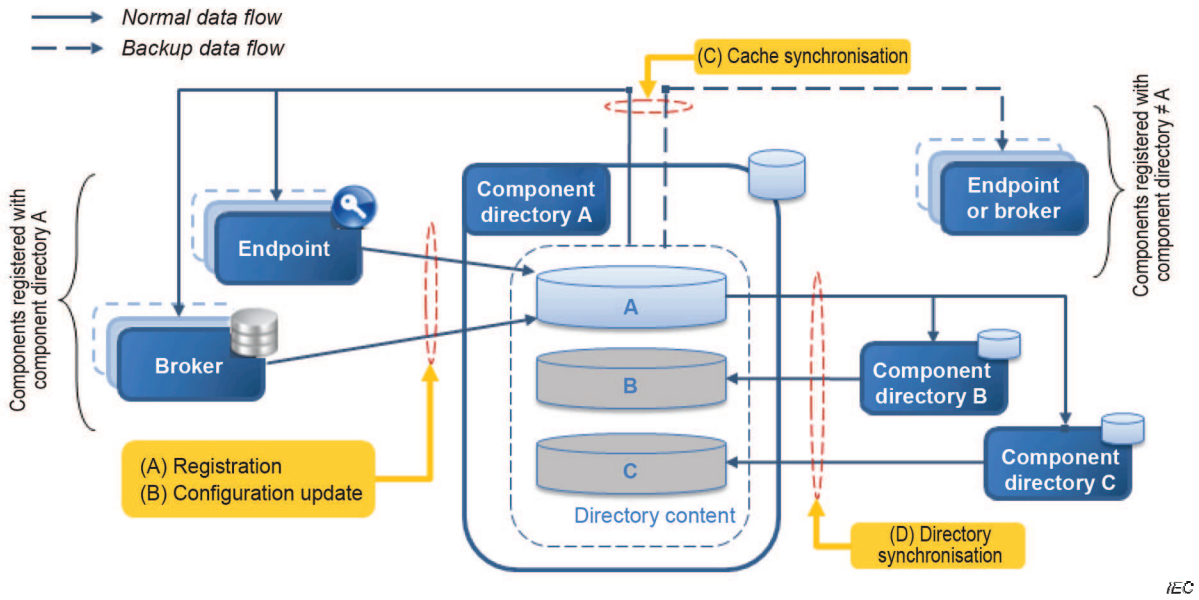

Figure 8 – Data flows with several component-directories

NOTE Locally caching the whole directory content is the key point for a component-directory not being critical in the system. The underlying design assumption is that, even when some hundred components compose the system, configuration data remains small and does not change frequently.

All services exposed by a component-directory are accessible using the https protocol as shown in Figure 9.

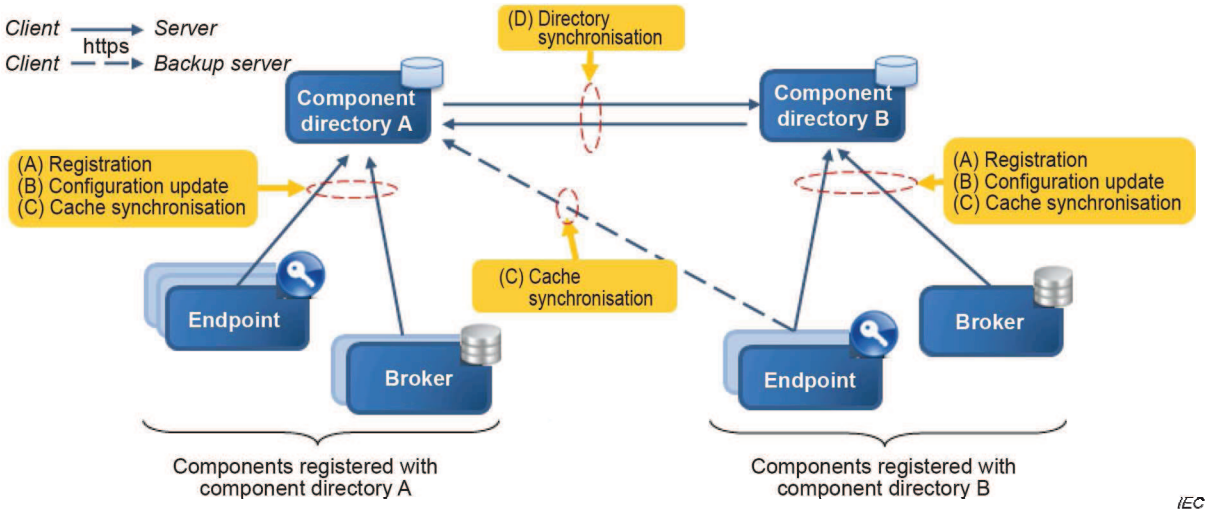

Figure 9 – Component-directory services and protocols

4.4.4 Interfaces exposed by the components

Figure 10 shows the interfaces that the specification defines in Clause 5, and that a compliant component implements, i.e. uses and exposes.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

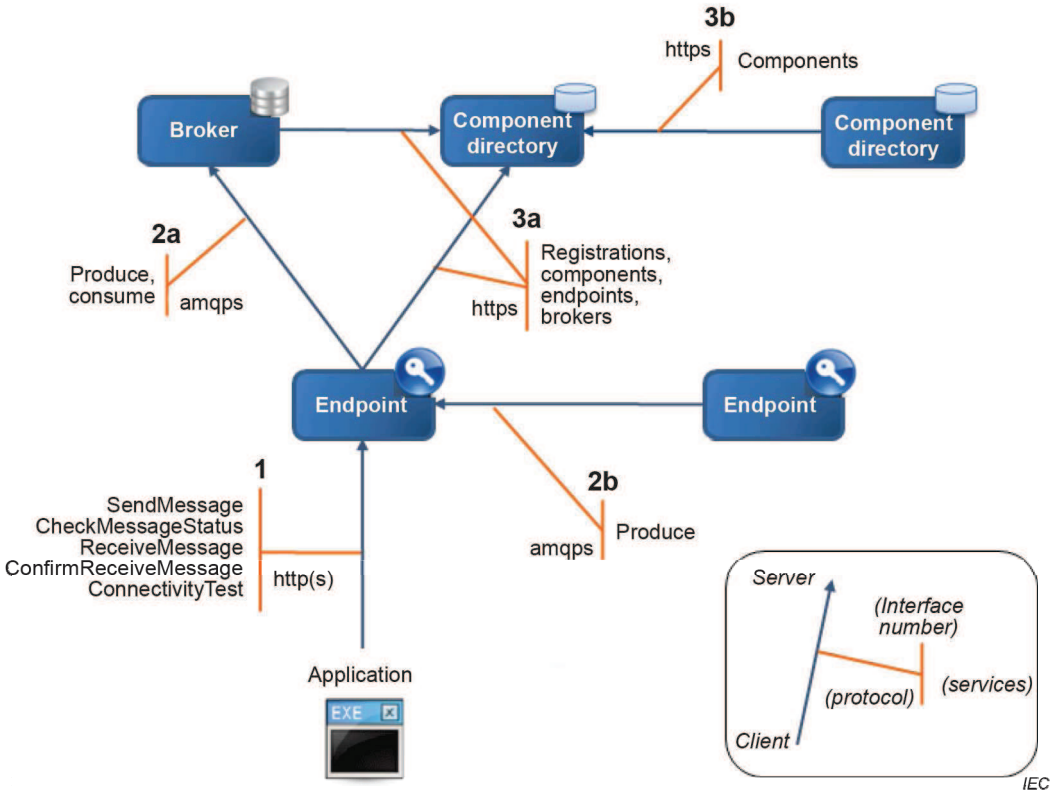

Figure 10 – MADES Interfaces, services and protocols

(1) Endpoint interface for applications using HTTP(S) SOAP web services – see 11.1.

- An application sends a message (*SendMessage*) through the system or requests for the delivery status of a previously sent message (*CheckMessageStatus*).
- An application requests for downloading a received message (*ReceiveMessage*) and then confirms back to the system that it has safely stored or processed the message (*ConfirmReceiveMessage*).

  NOTE Safe storage is defined in 5.9.
- An application requests the system to send a test message to a peer party (*ConnectivityTest*) in order to check that the communication with that party is working correctly for a given message-type.

(2a) Broker interface for endpoints using AMQP – see 6.3.

- AMQP is a protocol intended for the interoperability between various messaging middleware: it does not describe an interface but the byte-flow structure (*frames*) to exchange between two TCP peers (*on the wire*).
- A MADES broker is as a server that manages queues of (internal) messages until the intended recipient gets them.
- When successfully authenticated to the broker, an endpoint acts as a message producer to send a message (*Produce*) and as a message consumer to receive its intended messages (*Consume*).

(2b) Endpoint interface for others endpoints using AMQP – see 6.3.

- The interface for direct transfer between endpoints is the same as (2a) without the *Consume* service. Indeed, an endpoint does not contain queues in which other endpoints can consume messages.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

(3a) Component-directory interface used by endpoints and brokers – see 7.5.

- The endpoints and the brokers use the interface to register with their home directory-component into which they push configuration data. They also use the interface for keeping up-to-date a local copy of the system directory.
- The interface uses the REST principles. Requests and responses use XML format and are specified using XML schemas.
- The resources accessible to an authenticated component are:
  - *registrations*: to request for entering the system, to get and renew the certificates.
  - *components*: to get directory information about all components registered in the system in order to maintain a local copy of the directory. The answer returns either the whole directory content or nothing when the local directory is already up-to-date.
  - *endpoints* (resp. *brokers*): to get configuration data on an endpoint (resp. a broker) or to modify such information. Only a component can modify its own configuration data.

(3b) Component-directory interface used by other component-directories – see 7.5.

- A component-directory uses the interface to synchronise with another component-directory of the system.
- For synchronising, an "A" component-directory requests the *components* resources of a "B" component-directory exactly as endpoints and brokers do when using interface (3b). However, it only asks for the peer directory content restricted to the "B" subsystem components.

4.4.5 Architecture examples of MADES systems

A MADES system can range from a minimal architecture composed of two endpoints and one component-directory either without (Figure 11) or with a broker (Figure 12), up to a network of endpoints with several brokers and component-directories (Figure 13, Figure 14).

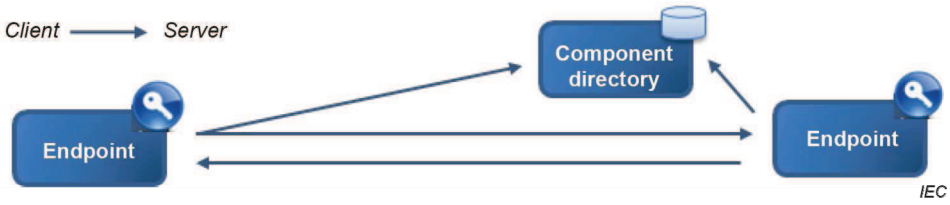

Figure 11 – Minimal MADES system (without broker)

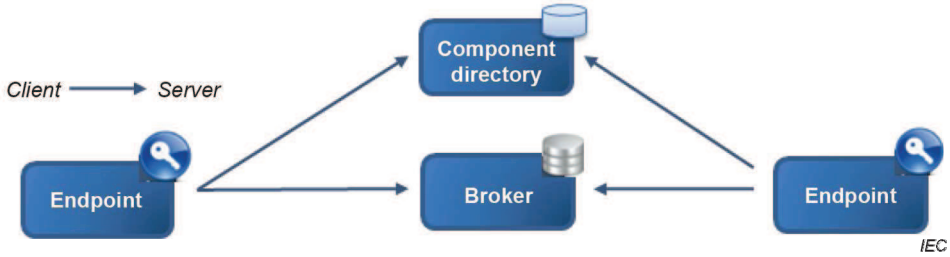

Figure 12 – Minimal MADES system (with broker)

Any of the two communicating parties using the architecture of Figure 12 can host either the broker or the component-directory or both.

A typical architecture is when one of the stakeholders of a business process, say "A", plays a central role (Figure 13). Therefore, he can host a broker and a component-directory. Acting as a hub in the business process logic, he also owns and hosts an endpoint for exchanging with other stakeholders.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11

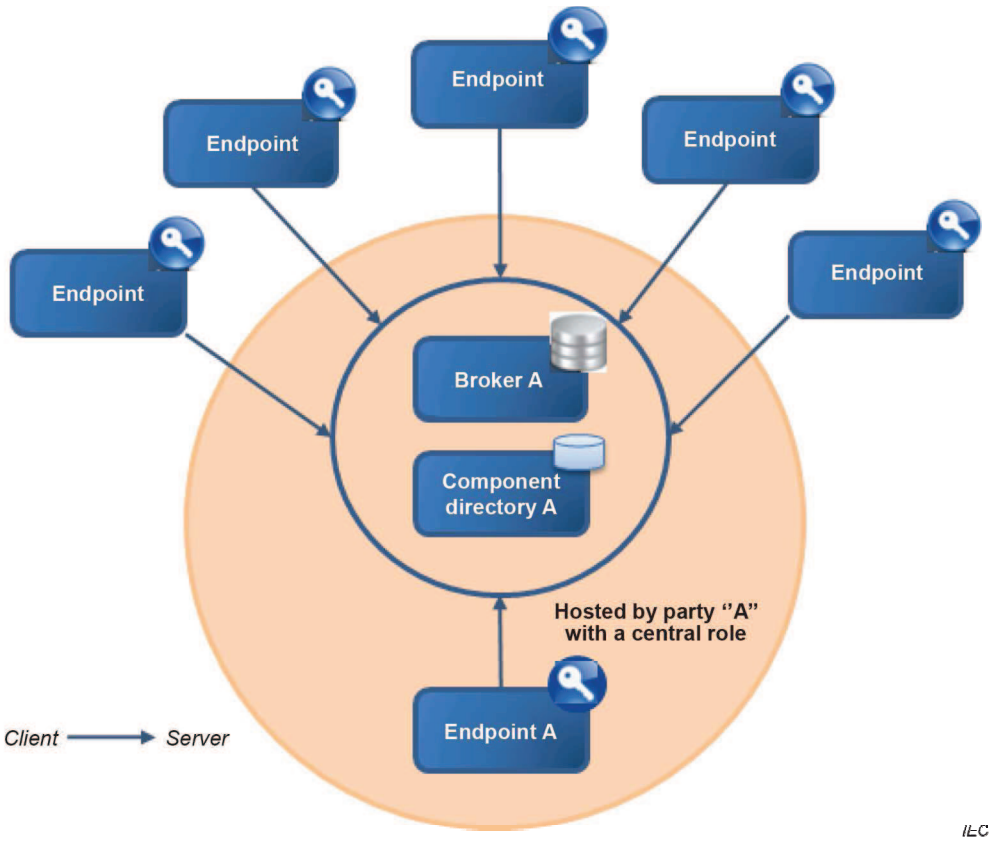

Figure 13 – MADES system with a party in a central role

Another business process could involve the same parties or others, or a subgroup, in which a party, say "B", now plays the central role. The parties can share the existing broker "A". But they also can use another and dedicated broker (broker "B") for reasons such as hosting localisation, business criticality, responsibility perimeter, contracted service-level agreement (SLA), project planning, etc., leading to a multi broker architecture as shown in Figure 14.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62325-503:2019-11

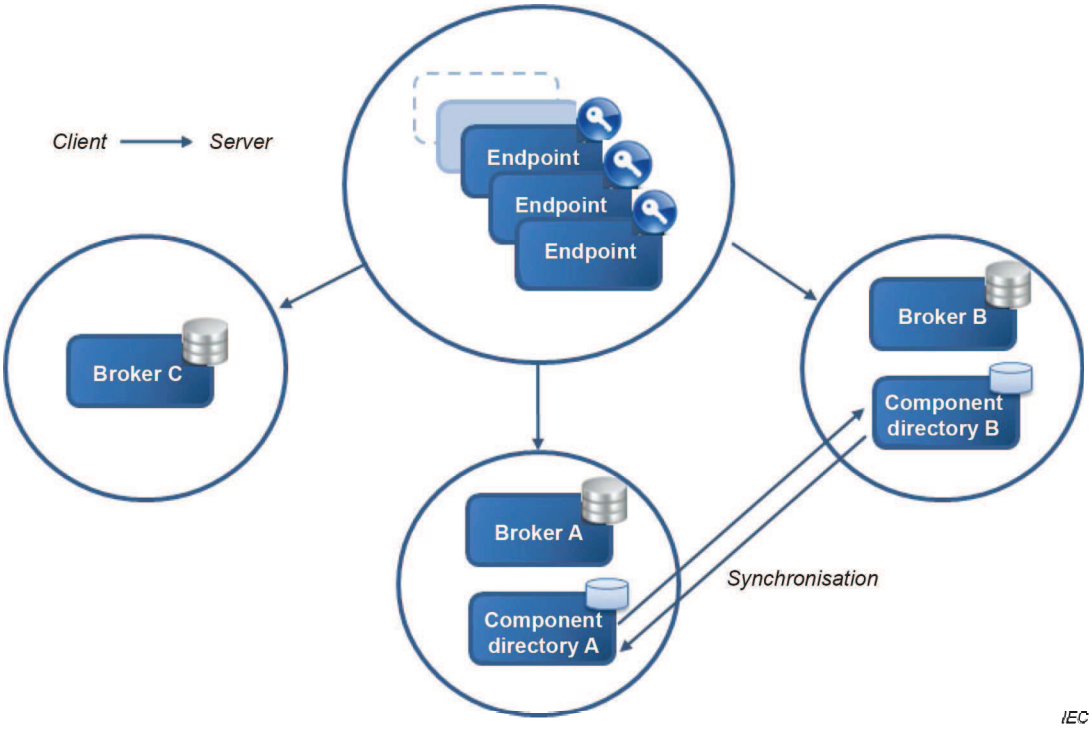

Figure 14 – MADES system with several brokers

Figure 14 shows two component-directories respectively hosted by parties who own broker A and broker B. There are two component-directories but possibly more. The rules are the following:

- Each component-directory synchronises with any other.
- The system has two component-directories. This is recommended for business continuity although the component-directory is not a critical component and could be down for some time without affecting the message delivery function.

In the Figure 14 example, both parties A and B host a component-directory and are registry offices each for a subsystem, i.e. a subset of endpoints and brokers of the system. However, the party C could also host a component-directory.

Figure 15 presents the same architecture viewed by a party involved in each business process. The party owns a single endpoint registered with a unique component-directory. Here the party accepts direct transfer and thus incoming connections to the endpoint. The architecture can encompass some direct bilateral exchanges between parties with no impact on the brokers.

Documents
Document Sharing Hub

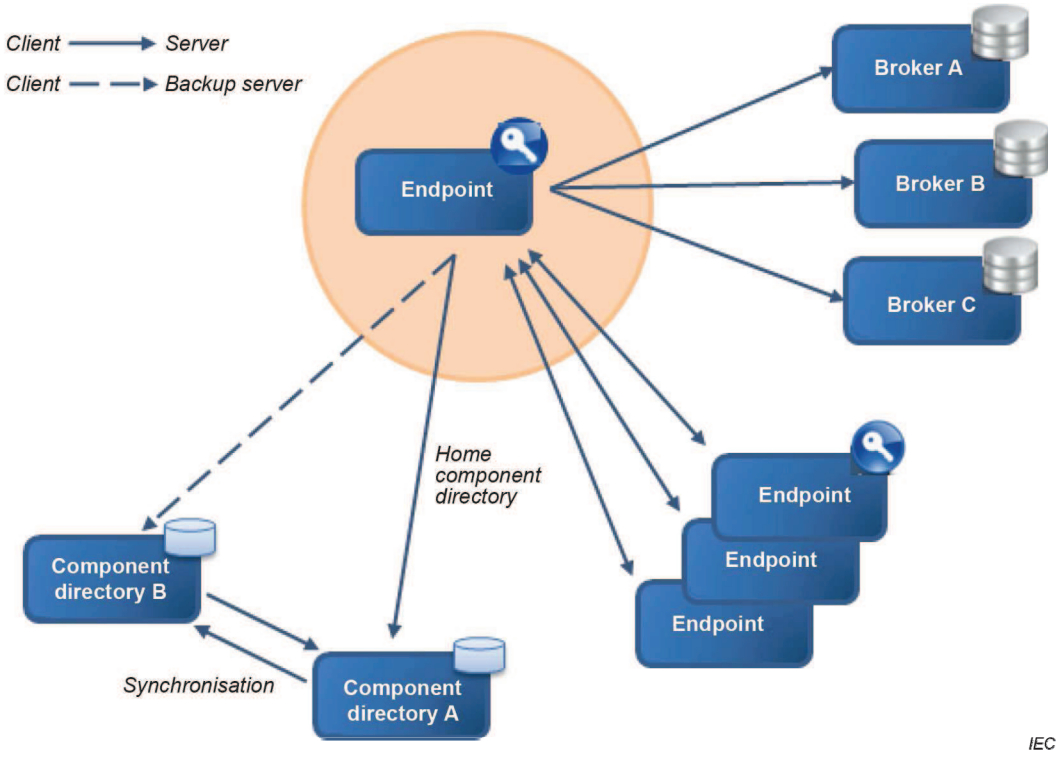

Figure 15 – Using a single endpoint for several business processes

The party could also choose to host multiple endpoints, each dedicated to a subset of business process or messages for reasons such as hosting localisation, business criticality, internal organisation and responsibility perimeter, contracted service-level agreement (SLA), project planning, etc. Each endpoint will then have to register with a component-directory, and the endpoints will appear in the system with different IDs as if owned by distinct parties. Such endpoints cannot behave in a master / slave mode, nor can they load balance the incoming message traffic towards the party[3].

4.5 Security and message integrity

4.5.1 Security goals and security solution

The goals of MADES security are:

- The security solution is transparent to applications – no specific implementation is required for an application to communicate securely.
- All communication channels are encrypted.
- Only the intended recipient can read a message.
- The recipient of a message can unambiguously identify the sender.
- Non-repudiation – A message together and its acknowledgement form an unambiguous proof that the sender sent the message and that the recipient received it.

The specified security solution complies with the X.509 public key infrastructure (PKI) using certificates, and it covers two security levels: a transport-layer security and a message-level security.

3 High availability of an endpoint is an issue of the endpoint design.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62325-503:2019-11