DIN EN IEC 62325-503

ICS 27.010; 35.240.50; 35.240.63

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

Gesamtumfang 93 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2018-08-30 angenommene Europäische Norm als DIN-Norm ist 2021-09-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN IEC 62325-503:2019-11.

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.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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

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.

Änderungen gegenüber der IEC-Vorgängerversion IEC TS 62325-503:2014:

a) Anwendung der Spezifikation ISO/IEC 19464:2014, Advanced Message Queuing Protocol (AMQP) v1.0;

b) Aufspaltung des in der IEC TS 62325-503:2014 beschriebenen Knotens in einen Broker, der die Nachrichtenzustellfunktion (en: Messaging-Funktion) implementiert, und ein Verzeichnis;

c) Erhöhung der Bedienbarkeit und Ausfallsicherheit des Kommunikationssystems durch die Möglichkeit für einen Endpunkt, Nachrichten über mehrere Broker zu senden und zu empfangen;

d) Vorteile der Standardisierung, Leistung und Skalierbarkeit des AMQP-Protokolls für die Übertragung von Nachrichten.

In diesem Dokument werden die folgenden Schriftarten verwendet:

Hilfe bei der Sichtbarkeit von Informationen in Tabelle und Diagramm: in kursiver Schrift ?? Kodierung in ASN.1 oder XACML: `couriernew`

Das Original-Dokument enthält Bilder und Schrift 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: DIN EN IEC 62325-503:2021-09

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN IEC 62325-503

Oktober 2018

ICS 33.200

Deutsche Fassung

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

(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)

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)

Diese Europäische Norm wurde von CENELEC am 2018-08-30 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

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

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

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Europäisches Vorwort

Der Text des Dokuments 57/1936/CDV, zukünftige 1. Ausgabe der IEC 62325-503, erarbeitet vom IEC/TC 57 „Power systems management and associated information exchange“ wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62325-503:2018 angenommen.

Nachstehende Daten wurden festgelegt:

– spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss	(dop):	2019-05-30
– spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen	(dow):	2021-08-30

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62325-503:2018 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Anhang ZA
(normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

Publikation	Jahr	Titel	EN/HD	Jahr
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: DIN EN IEC 62325-503:2021-09

Inhalt

Seite

Europäisches Vorwort ... 2

Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 3

Einleitung ... 10

1 Anwendungsbereich ... 11

2 Normative Verweisungen ... 11

3 Begriffe ... 11

4 Allgemeine Konzepte ... 13

4.1 Wozu dient MADES? ... 13

4.2 Überblick ... 14

4.3 Transparente und zuverlässige Nachrichtenzustellung ... 15

4.4 Komponenten eines MADES-Systems ... 16

4.4.1 Endpunkt-, Vermittler- und Komponentenverzeichnis ... 16

4.4.2 Zustellrouten und Bestätigungen ... 17

4.4.3 Teilen von Konfigurationsdaten des Systems ... 18

4.4.4 Von den Komponenten angezeigte Schnittstellen ... 20

4.4.5 Beispiele für die Architektur von MADES-Systemen ... 22

4.5 Sicherheit und Nachrichtenintegrität ... 25

4.5.1 Sicherheitsziele und Sicherheitslösung ... 25

4.5.2 Sicherheit der Transportschicht ... 26

4.5.3 Sicherheit der Nachrichtenschicht (message-level security): Signieren und Verschlüsseln ... 27

4.5.4 Unleugbarkeit ... 28

5 Zustellung der Nachrichten ... 30

5.1 Eindeutige Kennzeichnung von Komponenten und Nachrichten ... 30

5.2 Nachrichtentyp einer Nachricht ... 30

5.3 Nachrichtenroute zu einem Empfänger-Endpunkt: Nachrichtenpfade ... 30

5.4 Beschränkungen der Routen durch einen Vermittler ... 32

5.5 Annahme von Nachrichten durch einen Absender-Endpunkt ... 32

5.6 Nachverfolgung der Zustellung einer Nachricht ... 32

5.6.1 Nachrichtenstatus einer Nachricht ... 32

5.6.2 Zustellereignisse und Bestätigungen ... 33

5.7 Ablauf von Nachrichten ... 35

5.8 Zuverlässige Übertragung einer Nachricht ... 36

5.8.1 Erläuterungen ... 36

5.8.2 Übertragung zwischen Absender-Anwendung und Absender-Endpunkt ... 37

5.8.3 Übertragung zwischen Komponenten unter Verwendung des AMQP-Protokolls ... 38

5.8.4 Übertragung zwischen Empfänger-Endpunkt und Empfänger-Anwendung ... 38

5.9 Speichern interner Nachrichten in Komponenten ... 39

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Seite

5.10 Nachrichtenpriorität 39
5.11 Reihenfolge der Nachrichtenzustellung 39
5.12 Prüfen einer Route zwischen zwei Endpunkten: Nachverfolgungs-Nachrichten 40
6 Übertragung von Nachrichten unter Verwendung des AMQP-Protokolls 40
6.1 Grundprinzipien der AMQP-Spezifikation 40
6.1.1 Einleitung 40
6.1.2 Verbindung offen 41
6.1.3 Beginn der Sitzung 42
6.1.4 Anhängen einer Verknüpfung 42
6.1.5 Übertragung von Nachrichten 42
6.1.6 Wiederherstellung und erneutes Senden der Verknüpfung 42
6.1.7 Fehlermanagement 43
6.1.8 Nachrichtenstruktur 43
6.2 AMQP-Implementierung auf allgemeiner Ebene: das Client-/Vermittler-Modell 43
6.3 AMQP-Implementierung in MADES-Komponenten 44
6.4 Management von AMQP-Verbindungen und Anhängen durch einen Endpunkt 46
6.5 Internes Nachrichtenformat 47
6.5.1 Definitionen, Gestaltung und Sicherheitsprüfungen 47
6.5.2 AMQP-Format für die Übertragung interner Nachrichten 47
6.5.3 Verschlüsselung 48
6.5.4 Signieren 49
6.5.5 Metadaten der internen Nachricht 50
6.5.6 Beispiel-XML-Signatur 54
7 Management der Konfigurationsdaten des Systems 55
7.1 Erläuterungen 55
7.2 Verzeichnisinhalt und Eigentum der Informationen 55
7.3 Zur Konsistenz von Konfigurationsdaten 58
7.3.1 Konsistenz von Komponenten 58
7.3.2 Systemkonsistenz 58
7.3.3 Verteilte Implementierung von Updates 58
7.3.4 Eventuelle Konsistenz 59
7.4 Verbindung mit einem Komponentenverzeichnis 59
7.5 REST-API-Implementierung und verfügbare Ressourcen 59
7.6 Registrierungsprozess 61
7.7 Synchronisierungsprozess 62
7.7.1 Gültigkeitsdauer replizierter Daten: Restlebensdauer 62
7.7.2 Beschränkung des Synchronisationsflusses 62
7.7.3 Konfiguration des Synchronisierungsprozesses 63
7.8 XML-Schemata der API-Abfragen und Antworten 63

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Seite

7.8.1 Gemeinsame Typen ... 63
7.8.2 Registrierungsressource ... 66
7.8.3 Endpunkte, Vermittler und Komponentenressourcen ... 67
8 Handhabung der Zertifikate ... 68
8.1 Definitionen und Prinzipien ... 68
8.2 Zertifikate: Format und eindeutige ID ... 69
8.3 Verwendete Zertifikate und Zertifikat-Befugnisse der Aussteller ... 70
8.3.1 Überblick ... 70
8.3.2 Sicherheit der Transportschicht (Datenaustausch autorisieren) ... 70
8.3.3 Sicherheit der Nachrichtenschicht (Schutz der Vertraulichkeit von Nachrichten und Authentifizierung des Ausstellers der Nachricht) ... 71
8.4 Vertrauen in die Zertifikate anderer Komponenten ... 71
8.4.1 Authentifizierung ... 71
8.4.2 Signieren und Verschlüsselung ... 71
8.5 Verlängerung (nahezu) abgelaufener Zertifikate ... 71
8.6 Widerruf einer Komponente ... 72
9 Handhabung der Version der MADES-Spezifikation ... 72
9.1 MADES-Version dieses Dokuments ... 72
9.2 Ausgabe, Versionsbedeutung, Upgrade-Empfehlungen ... 72
9.3 Änderung der Signatur oder der Verschlüsselungs-Algorithmen ... 73
10 Administration und Betrieb der Komponenten ... 74
11 Schnittstelle für die Anwendungen ... 74
11.1 Endpunkt-Webservice-Schnittstelle für Anwendungen ... 74
11.1.1 Überblick ... 74
11.1.2 SendMessage-Dienst ... 75
11.1.3 ReceiveMessage-Dienst ... 76
11.1.4 ConfirmReceiveMessage-Dienst ... 78
11.1.5 CheckMessageStatus-Dienst ... 78
11.1.6 ConnectivityTest-Dienst ... 80
11.1.7 WSDL für die Webservice-Schnittstelle des Endpunkts ... 81
11.2 Gemeinsame Dateisystem-Ordner (FSSF, en: File System Shared Folders) ... 87
11.2.1 Überblick ... 87
11.2.2 Namenskonvention für Ordner und Dateien ... 88
11.2.3 Gleichzeitiger Zugriff auf Dateien ... 89
11.2.4 FSSF konfigurieren ... 90
Literaturhinweise ... 91

Bilder

Bild 1 – MADES-Übersicht ... 13

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Seite

Bild 2 – MADES Anwendungsbereich in einer geschichteten Architektur 14
Bild 3 – MADES-Nachrichtenzustellung 15
Bild 4 – MADES-Komponenten, -Interaktionen und -Protokolle 16
Bild 5 – Mögliche Routen für die Zustellung einer Nachricht 17
Bild 6 – Kommunikationsprotokolle für die Zustellung einer Nachricht 18
Bild 7 – Datenflüsse zwischen einem Komponentenverzeichnis und seinen registrierten Komponenten 19
Bild 8 – Datenflüsse mit mehreren Komponentenverzeichnissen 20
Bild 9 – Dienste und Protokolle des Komponentenverzeichnisses 20
Bild 10 – MADES-Schnittstellen, Dienste und Protokolle 21
Bild 11 – Minimales MADES-System (ohne Vermittler) 22
Bild 12 – Minimale MADES-System (mit Vermittler) 22
Bild 13 – MADES-System mit einer Partei in einer zentralen Rolle 23
Bild 14 – MADES-System mit mehreren Vermittlern 24
Bild 15 – Verwendung eines einzelnen Endpunkts für mehrere Geschäftsprozesse 25
Bild 16 – MADES-Transportsicherheit 26
Bild 17 – Sicherheit: geschützter Endpunkt 26
Bild 18 – Sicherheit: offenliegender Endpunkt 27
Bild 19 – Signieren von Nachrichten und Überprüfen der Signatur 27
Bild 20 – Verschlüsselung und Entschlüsselung von Nachrichten 28
Bild 21 – Keine Zurückweisung 29
Bild 22 – Nachrichtenstatus entlang der Lieferung 33
Bild 23 – Nachverfolgungsereignisse bei der Zustellung einer Nachricht 34
Bild 24 – Zuverlässige Übertragung 37
Bild 25 –Übertragung zwischen Absender-Anwendung und Absender-Endpunkt 37
Bild 26 – Übertragung zwischen dem Empfänger-Endpunkt und der Empfänger-Anwendung 38
Bild 27 – Die neun AMQP-Frames 41
Bild 28 – Struktur einer AMQP-Nachricht 43
Bild 29 – AMQP in MADES-Komponenten 45
Bild 30 – Zertifikate und Zertifizierungsstellen (CAs) eines MADES-Systems 70
Bild 31 – WSDL 1.1 Definitionen 81

Tabellen

Tabelle 1 – Eigenschaften der Nachverfolgungsereignisse 35
Tabelle 2 – Endgültiger Status einer Nachricht in einem Endpunkt 39
Tabelle 3 – Dienste des Client/Vermittler-Modells 44
Tabelle 4 – Regeln für das Einrichten von Verbindungen/Anhängen und die Nachrichtenübertragung 46
Tabelle 5 – Interne Nachricht – AMQP-Format: Header-Abschnitt 47
Tabelle 6 – Interne Nachricht – AMQP-Format: Eigenschaften-Abschnitt 48

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Seite

Tabelle 7 – Interne Nachricht – AMQP-Format: Anwendungseigenschaften-Abschnitt 48
Tabelle 8 – Interne Nachricht – AMQP-Format: Anwendungsdaten-Abschnitt 48
Tabelle 9 – Verschlüsselung – Verarbeitungsmetadaten-Attribute für die „AES-256“-Chiffre 49
Tabelle 10 – Signieren – Verarbeitungsmetadaten-Attribute für den „SHA-512“-Algorithmus 50
Tabelle 11 – Nachrichten-Metadaten (Typ) 51
Tabelle 12 – InternalMessageType (Typ: String-Aufzählung) 52
Tabelle 13 – ProcessingMetadata (Typ) 52
Tabelle 14 – MessageProcessor (Typ) 52
Tabelle 15 – Karte (Typ) 52
Tabelle 16 – MapEntry (Typ) 52
Tabelle 17 – ValueType (Typ: String-Aufzählung) 53
Tabelle 18 – Komponentenverzeichnis – Inhalt eines Eintrags 56
Tabelle 19 – Zertifikat (Typ) 57
Tabelle 20 – MadesImplementation (Typ) 57
Tabelle 21 – MessagePath (Typ) 57
Tabelle 22 – BrokerRestriction (Typ) 57
Tabelle 23 – HTTP-Operationen 59
Tabelle 24 – HTTP-Rückgabecodes 60
Tabelle 25 – Komponentenverzeichnis-API 61
Tabelle 26 – Endpunkt-Schnittstelle – Allgemeiner Fehler 75
Tabelle 27 – Endpunkt-Schnittstelle – Wert für errorCode 75
Tabelle 28 – SendMessage – Abfrageelemente 75
Tabelle 29 – SentMessage (Typ) 76
Tabelle 30 – SendMessage – Antwortelemente 76
Tabelle 31 – SendMessage – Weitere Fehlerelemente 76
Tabelle 32 – ReceiveMessage – Abfrageelemente 77
Tabelle 33 – ReceiveMessage – Antwortelement 77
Tabelle 34 – ReceivedMessage (Typ) 77
Tabelle 35 – ReceiveMessage – Weitere Fehlerelemente 77
Tabelle 36 – ConfirmReceiveMessage – Abfrageelemente 78
Tabelle 37 – ConfirmReceiveMessage – Antwortelement 78
Tabelle 38 – ConfirmReceiveMessage – Weitere Fehlerelemente 78
Tabelle 39 – CheckMessageStatus – Abfrageelemente 79
Tabelle 40 – CheckMessageStatus – Antwortelemente 79
Tabelle 41 – MessageStatus (Typ) 79
Tabelle 42 – MessageTraceItem (Typ) 79
Tabelle 43 – MessageState oder MessageTraceState (Typ: String-Aufzählung) 80
Tabelle 44 – CheckMessageStatus – Weitere Fehlerelemente 80
Tabelle 45 – ConnectivityTest – Abfrageelemente 80

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

Seite

Tabelle 46 – ConnectivityTest – Antwortelemente 80
Tabelle 47 – ConnectivityTest – Weitere Fehlerelemente 80
Tabelle 48 – FSSF – Ordner- und Dateinamenformat 88
Tabelle 49 – FSSF – Zur Generierung der Dateinamen verwendete Token 89

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

Einleitung

Dieses Dokument ist Teil der Normenreihe IEC 62325 für Kommunikation im deregulierten Energiemarkt.

Hauptziel der Normenreihe IEC 62325 ist es, Dokumente zu schaffen, die die Integration von unabhängig von verschiedenen Lieferanten entwickelter Marktanwendungssoftware in ein Marktmanagementsystem, zwischen Marktmanagementsystemen und Marktteilnehmersystemen, erleichtert. Dies wird durch die Festlegung des Nachrichtenaustauschs erreicht, um diesen Anwendungen oder Systemen den Zugang zu öffentlichen Daten und den Informationsaustausch, unabhängig von der internen Informationsdarstellung, zu ermöglichen.

Das allgemeine Informationsmodell (CIM, en: common information model) legt die Semantikbasis für den Nachrichtenaustausch fest. IEC 62325−351 legt die europäischen Marktprofiltyp-Spezifikationen fest, die die geplanten europäischen Strommärkte unterstützen. Diese Strommärkte basieren auf den Europäischen Vorschriften und den Konzepten des Zugriffs Dritter und zonaler Märkte. Die internationalen Dokumente der Normenreihe IEC 62325-451-n legen den Inhalt der ausgetauschten Nachrichten fest.

Der Zweck dieses Dokuments ist es, die Richtlinien für den Austausch der vorgenannten Nachrichten bereitzustellen. Ein europäischer Marktteilnehmer (Händler, Verteilungsunternehmen usw.) könnte von einer einzigen, gemeinsamen, harmonisierten, sicheren Plattform für den Nachrichtenaustausch mit den europäischen Übertragungsnetzbetreibern (ÜNB) profitieren; dadurch würden die Kosten für den Aufbau verschiedener IT-Plattformen als Schnittstelle zu allen beteiligten Parteien gesenkt.

Dieses Dokument ist ein wichtiger Schritt in der Unterstützung von in die Strommärkte eintretenden Parteien, die keine staatlichen Parteien sind; diese könnten dasselbe oder ein ähnliches Informationsaustauschsystem nutzen, um an mehr als einem Markt in ganz Europa teilzunehmen.

Dieses Dokument basierte ursprünglich auf der Arbeit der Arbeitsgruppe EDI des Verbands der Europäischen Übertragungsnetzbetreiber (ENTSO-E, en: European Network of Transmission System Operators).

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

1 Anwendungsbereich

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

Dieses Dokument legt einen Standard für eine Kommunikationsplattform fest, mit dem jeder Übertragungsnetzbetreiber (TSO, en: Transmission System Operator) in Europa zuverlässig und sicher Dokumente für den Energiemarkt austauschen kann. Folglich könnte ein europäischer Marktteilnehmer (TSO, regionales Kontrollzentrum, Verteilnetz, Strombörse usw.) von einer einzigen, gemeinsamen, harmonisierten und sicheren Plattform für den Nachrichtenaustausch mit anderen Teilnehmern profitieren; d. h. von der Reduzierung der Kosten für den Aufbau verschiedener Informationstechnologie-(IT)-Plattformen zur Verbindung mit allen beteiligten 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 internationalen IT-Standards:

- Aus Sicht des Anwendungsprogramms legt MADES die Softwareschnittstellen für den Austausch elektronischer Dokumente mit Peer-Anwendungen fest. 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 den Status der Zustellung eines Dokuments abfragen und der Empfänger sendet eine Nachricht, d. h. die Bestätigung, beim Empfang des Dokuments zurück. Dies macht ein MADES-System verwendbar für den Austausch von Dokumenten in Geschäftsprozessen, die eine zuverlässige Lieferung erfordern.
- MADES legt auch Dienste fest, die für die Anwendungen versteckt sind, wie z. B. Empfängerlokalisierung, Empfängerverbindungsstatus, Nachrichtenweiterleitung und Sicherheit. Die Dienste beinhalten ein Verzeichnis, Authentifizierung, Signierung, Verschlüsselung, Nachrichtenverfolgung, Nachrichtenprotokollierung und Nachrichten-Zwischenlagerung.

Zweck von MADES ist es, einen sicheren Nachrichtenaustauschstandard auf der Grundlage von Standardkommunikationsprotokollen und unter Nutzung der besten IT-Praktiken für den Datenaustausch über TCP/IP-Kommunikationsnetzwerke zu schaffen, um den Business-to-Business (B2B)-Informationsaustausch nach den Normenreihen IEC 62325-351 und IEC 62325-451 zu unterstützen.

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

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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*

3 Begriffe

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

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

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

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, abgesichert durch die Sicherheit der Transportschicht
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 Abfragen des Zugriffs und Handhabung textlicher 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 Webservice

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 Sicherstellung der Privatsphäre und Datenintegrität zwischen zwei kommunizierenden Computeranwendungen

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62325-503:2021-09

4 Allgemeine Konzepte

4.1 Wozu dient MADES?

ANMERKUNG Abschnitt 4 beschreibt den Geschäftskontext für die Nutzung der Spezifikation, stellt die Hauptkonzepte der Spezifikation vor und enthält keine Anforderungen.

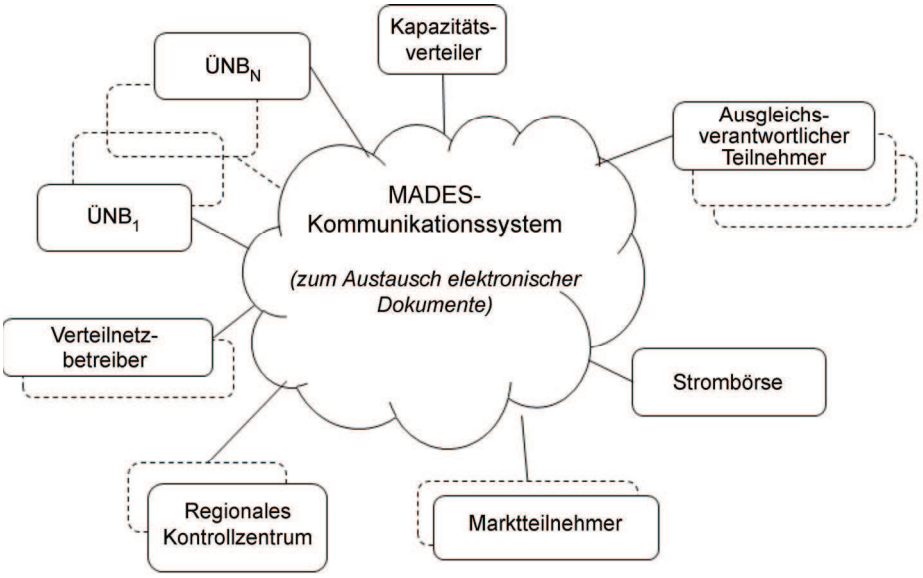

Bild 1 – MADES-Übersicht

MADES dient in erster Linie dazu, Übertragungsnetzbetreibern (ÜNB) ein genormtes Kommunikationssystem für den sicheren Austausch elektronischer Dokumente untereinander und mit anderen Parteien auf dem europäischen Strommarkt, wie in Bild 1 gezeigt, zu bieten.

Diese Dokumente sind hauptsächlich für den Energiemarkt verwendete Dokumente und in den Normenreihen IEC 62325-351und IEC 62325−451 beschrieben. Solche Parteien umfassen ÜNB, regionale Kontrollzentren, Strombörsen, Verteilnetzbetreiber, für den Marktausgleich verantwortliche Parteien, Übertragungskapazitätsverteiler, Marktbetreiber, Kapazitätshändler, Erzeuger usw.

MADES ermöglicht es jeder Partei, über einen Zugangspunkt zu dem Kommunikationssystem zu verfügen: Anwendungen dieses Kommunikationssystems können den Zugangspunkt dann nutzen, um sicher Dokumente anderen Parteien zu senden und von ihnen zu empfangen.

Technisch gesehen ist MADES ein Datenaustausch-Standard, der aus Standardkommunikationsprotokollen besteht und Normen und beste Praktiken der Informationstechnologie nutzt, um einen Mechanismus für den Austausch von Daten über jedes TCP/IP-Kommunikationsnetzwerk und jede Infrastruktur zu entwickeln und den Informationsaustausch zwischen Unternehmen zu ermöglichen.

Neue Marktregeln führen zu neuen Geschäftsprozessen und Aktivitäten und erfordern im Allgemeinen einen neuen Informationsaustausch zwischen den Parteien. Die Erfahrung zeigt, dass die gewählte technische Lösung für einen Datenaustausch, der die Ziele der Unternehmen erfüllt, aus einer Vereinbarung aller beteiligten Parteien unter Erfassung verschiedener Beschränkungen einschließlich des Implementierungszeitrahmens, der Angebote der Lieferanten, der bereits bestehenden Kommunikationsinfrastruktur und -verbindungen, der Integrationsfähigkeiten bestehender Informationssysteme, der Vertraulichkeit der ausgetauschten Informationen, der rechtlichen Risiken, der Leistung usw. resultiert.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

Wo Geschäftsprozesse den Austausch zwischen mehreren Systemen oder Parteien erfordern, können bilateral entwickelte Lösungen komplex werden, da jede Schnittstelle Zeit benötigt, bis sie in Betrieb genommen werden kann, und die Entwicklung und Instandhaltung Zeit und Ressourcen kostet. Eine auffällige Konsequenz ist, dass einige an den Geschäftsprozessen beteiligte Parteien, die den Austausch mit anderen Parteien erfordern, gegebenenfalls andere Kommunikationstools und -lösungen für die Verbindung mit mehreren Informationssystemen installieren und betreiben müssen. Der Weg zu einem besser integrierten europäischen Strommarkt führt zu vielen solcher Situationen mit neu koordinierten Prozessen zwischen Akteuren mit regulierten Rollen. Auch die Marktteilnehmer in mehreren Ländern wünschen sich eine harmonisierte Schnittstelle.

MADES kann jeden Geschäftsprozess ungeachtet des übertragenen Dokumentenformats (z. B. XML, binär) und der Austauschsequenz unterstützen.

MADES ist unabhängig von der zugrundeliegenden Kommunikationsinfrastruktur, die aus einem Internetprotokoll-(IP)-Netzwerk wie etwa Internet, einer privaten physischen Infrastruktur oder einem virtuellen privaten Netz (VPN) mit mehreren Zugangspunkten bestehen kann.

MADES basiert ausschließlich auf nicht-proprietären IT-Standards für Kommunikationsprotokolle, Datenintegrität, Peer-Authentifizierung (Signatur), Vertraulichkeit (Verschlüsselung), Verzeichnis der zugänglichen Parteien (z. B. HTTP, AMQP, TLS, X.509), wie in Bild 2 gezeigt.

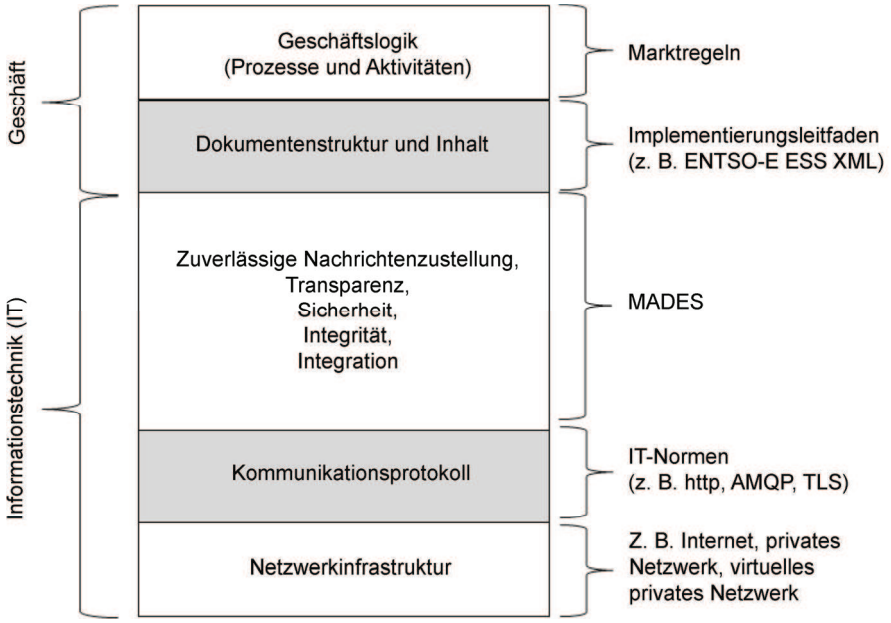

Bild 2 – MADES Anwendungsbereich in einer geschichteten Architektur

4.2 Überblick

Der MADES-Standard legt ein Kommunikationssystem fest, das Nachrichten zwischen autorisierten Parteien liefert. Ein solches System weist die folgenden wesentlichen Eigenschaften auf:

1) Zuverlässige Nachrichtenzustellung – Eine verbundene (Absender-) Partei kann eine Nachricht an eine andere verbundene (Empfänger-) Partei oder eine Partei, die sich mit dem System verbinden kann, senden. Der Absender wird benachrichtigt, wenn eine Nachricht aus irgendeinem Grund nicht zeitnah von dem Empfänger bestätigt wird.
2) Transparenz – Das System ist keine Blackbox: Es verfolgt jede Nachricht, um vertrauenswürdige Informationen über die Zustellung zu sammeln.
3) Sicherheit – Nur der Empfänger der Nachricht kann den Inhalt lesen (Vertraulichkeit) und der Empfänger authentifiziert den Absender (Signatur) eindeutig.
4) Integrität – Das System garantiert, dass der Inhalt einer Nachricht während des Zustellungsprozesses nicht verändert wird.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

5) Integration – Eine Vielzahl unterschiedlicher Technologien kann die offengelegten Dienste für das Senden und Empfangen von Nachrichten integrieren. Dies erleichtert die Entwicklung und Integration in jedes Informationssystem.

Die ersten vier Hauptmerkmale (zuverlässige Nachrichtenzustellung, Transparenz, Sicherheit und Integrität) sind Fähigkeiten des Systems, während die letzte (Integration) ein Designmerkmal der MADES-Komponenten ist.

4.3 Transparente und zuverlässige Nachrichtenzustellung

Die Nachrichtenzustellungsfunktion ist das Hauptmerkmal eines MADES-Systems, wie in Bild 3 gezeigt.

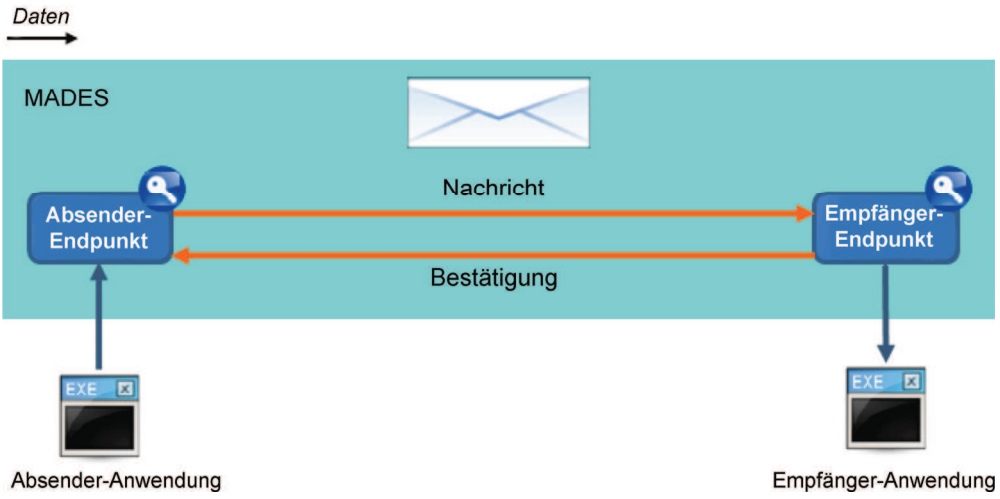

Bild 3 – MADES-Nachrichtenzustellung

Ein Absender möchte oder muss ein Dokument mithilfe des Systems an einen Empfänger übertragen. Der Absender und der Empfänger sind beide Anwendungen, die eine Anwendungsprogrammierschnittstelle (API, en: application programming interface) nutzen, um sich mit ihren als *Endpunkten* bezeichneten jeweiligen Zugangspunkten zu verbinden.

Die Peer-Anwendungen sehen das System nur durch die definierte Schnittstelle. Das zwischen den Parteien übertragene Dokument kann aus Text oder binären Daten bestehen. Tatsächlich überträgt das System eine Nachricht, die das Dokument mit zusätzlichen Metadaten mit Informationen für sicheres Routing und Übertragen der Nachricht wie etwa eine eindeutige ID, die Identitäten der Peer-Endpunkte und Verschlüsselungsinformationen in Verbindung mit der Unterzeichnung der Nachricht und der Verschlüsselung des Dokuments enthält.

Das System verfolgt jede Nachricht, die ein Empfänger-Endpunkt akzeptiert hat. Der Endpunkt kann eine Abfrage aus einer Business-Anwendung für die Versendung eines Dokuments ablehnen, z. B. wenn der Empfänger unbekannt ist.

Die Absender-Anwendung kann jederzeit den Status einer gesendeten Nachricht als AKZEPTIERT, ZUGESTELLT, EMPFANGEN oder FEHLGESCHLAGEN überprüfen (siehe 5.6.1).

Der Absender-Endpunkt weiß, dass das System eine Nachricht an den Empfänger-Endpunkt zugestellt hat, wenn er eine Bestätigung von dem Empfänger-Endpunkt erhält. Der Absender-Endpunkt setzt den Status der Nachricht auf FEHLGESCHLAGEN, wenn die Nachricht abläuft, d. h. wenn er aus irgendeinem Grund keine zeitnahe Bestätigung erhält.

Das System überträgt:

- Standardnachrichten – eine Nachricht, die von einem Absender-Endpunkt erstellt wird, um ein elektronisches Dokument auf Abfrage einer Absender-Anwendung zu versenden.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

- Bestätigung – eine von einem Empfänger-Endpunkt erstellte Nachricht, um die Zustellung[1] einer Standardnachricht zwischen Endpunkten nachzuverfolgen. Die Anwendungen wissen nichts über die Bestätigungen, die intern im System verbleiben.

ANMERKUNG Das einzelne Wort „Nachricht“ bezieht sich im weiteren Verlauf des Dokuments auf „Standardnachricht“ und „interne Nachricht“ bezieht sich allgemein auf eine (Standard-) Nachricht oder eine Bestätigung.

4.4 Komponenten eines MADES-Systems

4.4.1 Endpunkt-, Vermittler- und Komponentenverzeichnis

Ein MADES-System besteht aus drei Arten von Komponenten: Endpunkt, Broker und Komponentenverzeichnis. Zwei Komponenten interagieren in einer Client/Server-Betriebsart, wie in Bild 4 gezeigt. Dies ist die Vollansicht, die in dem vorliegenden Abschnitt im Einzelnen erläutert wird.

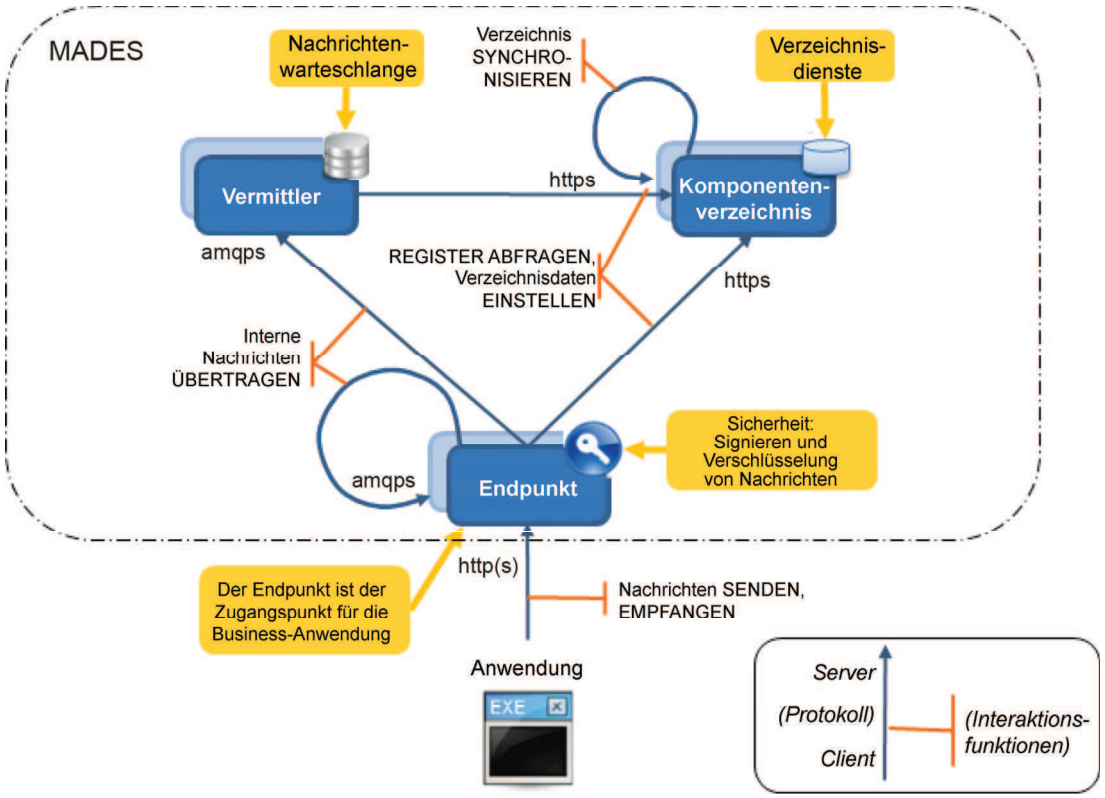

Bild 4 – MADES-Komponenten, -Interaktionen und -Protokolle

Eine Partei, die das System nutzt, verfügt über einen Endpunkt. Eine Anwendung (*Client*) nutzt die von dem Endpunkt angezeigte Schnittstelle (*Server*), um Nachrichten zu senden und zu empfangen. Die Schnittstelle nutzt das HTTP(S)-Protokoll.

ANMERKUNG Die Client-Komponente öffnet eine Verbindung. Die Server-Komponente akzeptiert die Verbindung.

Dieses Dokument verweist auf einen Sender-(oder Empfänger-)Endpunkt, wenn es sich auf die Operationen konzentriert, die ein Endpunkt durchführt, um eine Nachricht zu versenden (oder zu empfangen). Die Endpunkte sind für die komplette Sicherheit verantwortlich, d. h. der Absender-Endpunkt signiert und verschlüsselt die Nachricht, während der Empfänger die Nachricht entschlüsselt und die Signatur des Absenders überprüft.

[1] Dies ist eine technische Bestätigung und keine Bestätigung nach IEC 62325-451-1.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

Der Absender-Endpunkt (*Client*) lädt die Nachricht zur Übertragung auf einen Vermittler (*Server*) hoch und der Empfänger-Endpunkt (*Client*) lädt die Nachricht von diesem Vermittler herunter. Der Vermittler speichert die Nachricht vorübergehend in einer Warteschlange. Dieser Vorgang wird im weiteren Verlauf als *indirekte* Übertragung bezeichnet. Der Absender-Endpunkt (*Client*) kann die Nachricht darüber hinaus direkt in den Empfänger-Endpunkt (*Server*) hochladen: Dies wird im weiteren Verlauf als *direkte* Übertragung bezeichnet. Das Protokoll zur Übertragung der Nachricht lautet ungeachtet der Route AMQPS (en: Advanced Message Queuing Protocol Secured) mit Sicherheit der Transportschicht (TLS).

Die Übertragung der Bestätigung funktioniert auf dieselbe Weise, allerdings tauschen die Peer-Endpunkte die Rolle, der Empfänger fungiert als Absender und umgekehrt. Ein Vermittler arbeitet nur mit internen Nachrichten und unterscheidet nicht zwischen Nachrichten und Bestätigungen.

Die Endpunkte und die Vermittler (*alle Clients*) erhalten die Konfigurationsdaten des Systems, z. B. die Identifikationen der bestehenden Komponenten, Zertifikate, autorisierte Zustellrouten, aus einem Komponentenverzeichnis (*einem Server*), das ein Adressbuch implementiert. Wenn das System mehrere Komponentenverzeichnisse umfasst, synchronisieren diese sich gegenseitig. Die Verzeichnisdienste nutzen das HTTPS-Protokoll.

4.4.2 Zustellrouten und Bestätigungen

Bild 5 zeigt die möglichen Routen zur Übertragung einer Nachricht:

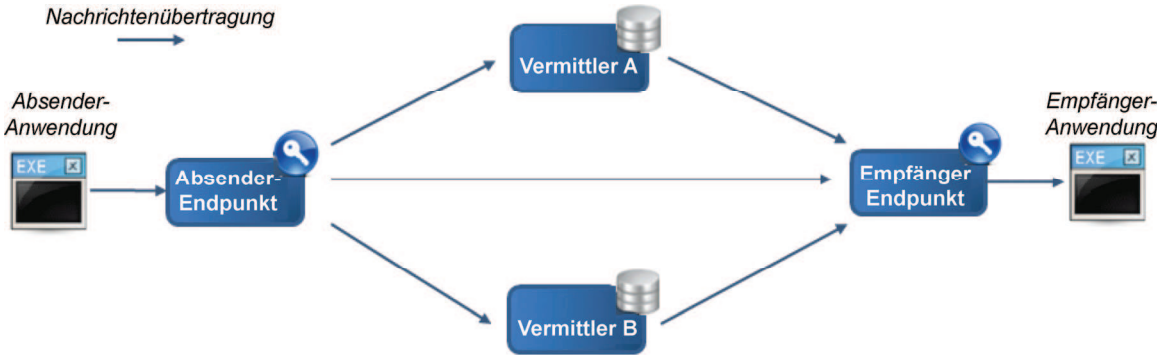

Bild 5 – Mögliche Routen für die Zustellung einer Nachricht

Ein Absender-Endpunkt kann eine Nachricht entweder über einen zwischengeschalteten Vermittler oder direkt an einen Empfänger-Endpunkt übertragen. Die Aktivierung oder Nichtaktivierung einer direkten Übertragung ist eine Frage der Sicherheit (siehe 4.5.2).

Bild 5 zeigt, dass das System mehrere Vermittler enthalten kann und Nachrichten zwischen zwei Endpunkten verschiedene Routen nutzen können. Die Route richtet sich nach der Art des zu übertragenden Dokuments, die nach dem *Nachrichtentyp* benannt ist, der die Nachricht grundsätzlich an bestimmte Geschäftsprozesse bindet (siehe 5.2). Der Absender-Endpunkt wählt die Route entsprechend dem Nachrichtenpfad (siehe 5.3) in Verbindung mit dem Nachrichtentyp, wie durch den *Empfänger*-Endpunkt konfiguriert und in den Komponentenverzeichnissen veröffentlicht und verfügbar.

Bild 6 zeigt die entlang der Nachrichtenroute verwendeten Kommunikationsprotokolle.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

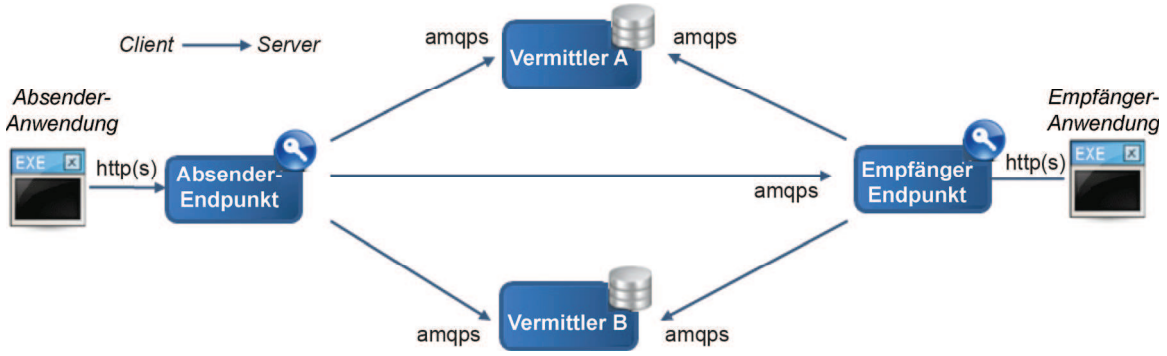

Bild 6 – Kommunikationsprotokolle für die Zustellung einer Nachricht

Eine Bestätigung ist eine von dem Empfänger-Endpunkt zurück an den Absender-Endpunkt ausgegebene Bestätigung des Empfangs einer Nachricht. Die Route der Bestätigung entspricht *genau der umgekehrten Route* der entsprechenden Nachricht.

ANMERKUNG

- Die Absender-Anwendung legt den Nachrichtentyp fest, wählt aber nicht die Route aus. Die Änderung des Nachrichtenpfads verändert die Route, beeinflusst aber nicht die Anwendungen.
- Ein Lastausgleich des Nachrichtenverkehrs über mehrere Vermittler ist nicht möglich. Alle Nachrichten desselben Nachrichtentyps zwischen zwei gegebenen Endpunkten verwenden dieselbe Route. Einige Vermittler können Cluster-Konfigurationen mit hoher Verfügbarkeit unterstützen.
- Es besteht maximal ein Vermittler auf der Route von einem Absender-Endpunkt zu einem Empfänger-Endpunkt.

4.4.3 Teilen von Konfigurationsdaten des Systems

Die transparente Implementierung des Nachrichten-Routings und der Sicherheit in Anwendungen führt dazu, dass die Endpunkte und Vermittler auf die Konfigurationsdaten, die das System beschreiben, zugreifen. Dies umfasst die folgenden Informationen für jede Komponente:

- eindeutige ID,
- Sicherheitszertifikate für die Authentifizierung, Unterzeichnung und Verschlüsselung,
- Standort des Telekommunikationsnetzwerks für den Zugriff auf die von der Komponente angezeigten Dienste,
- Regeln für die Nachrichtenzustellung: für einen Endpunkt bestimmen die Regeln die Routen für das Senden der Nachricht an den Endpunkt und für einen Vermittler, welche Nachrichten der Vermittler akzeptiert, d. h. welche Nachrichtentypen und von welchen Absender-Endpunkten,
- betriebliche Kontaktinformationen.

Jeder Endpunkt und jeder Vermittler wird in einem einzelnen Komponentenverzeichnis eingetragen, das nach seinem *Home-Komponentenverzeichnis* benannt ist. Eine wesentliche Aufgabe des Administrators eines Komponentenverzeichnisses besteht darin, neue Parteien zu akzeptieren, ihre Vertrauenswürdigkeit festzustellen und ihre Komponenten zu registrieren. Die Rolle beinhaltet die umgekehrten Operationen: das Austragen von Komponenten und insbesondere von potentiell manipulierten Komponenten. Ein Komponentenverzeichnis und seine eingetragenen Komponenten bilden ein *Teilsystem*.

Bild 7 zeigt Datenflüsse zwischen einem Komponentenverzeichnis „A“ und seinen eingetragenen Komponenten:

(A) Wenn es eine Registrierungsabfrage akzeptiert, erstellt das Komponentenverzeichnis einen neuen Eintrag für die Komponente in dem Verzeichnis. Darüber hinaus erstellt und speichert es die Komponentenzertifikate.

(B) Der Administrator einer eingetragenen Komponente gibt alle Konfigurationsdaten der Komponenten ein, die per Push-Nachricht im Home-Komponentenverzeichnis aktualisiert werden.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

(C) Eine registrierte Komponente speichert lokal den gesamten Verzeichnisinhalt in einem Cache-Speicher und fordert regelmäßig eine Synchronisierung an. Bei einer Veränderung erhält sie eine vollständige Kopie des Verzeichnisses und nicht nur die schrittweisen Änderungen.

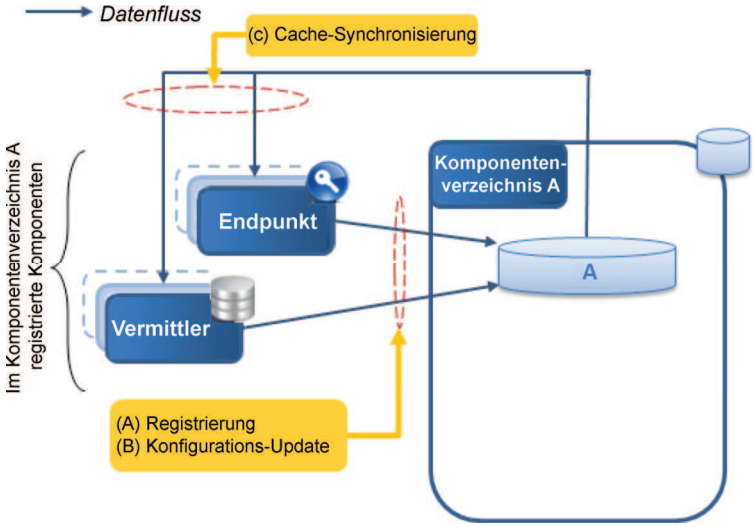

Bild 7 – Datenflüsse zwischen einem Komponentenverzeichnis und seinen registrierten Komponenten

Die Spezifikation des Komponentenverzeichnisses dient zwei Zwecken:

1) Minimierung administrativer Aufgaben: die Dateneingabe wird begrenzt. Darüber hinaus und weil die erste Registrierung wahrscheinlich immer eine manuelle Annahme erfordern sollte, könnten die Zertifikate[2] automatisch verlängert werden (siehe 7.6), wenn die Abfrage von einer gültig eingetragenen Komponente stammt.
2) Gestaltung einer nichtkritischen Komponente, d. h. die bei einem Ausfall die Nachrichtenübertragung nicht blockiert. Jeder Endpunkt und jeder Vermittler speichert und aktualisiert Verzeichnisdaten lokal in einem Cache-Speicher. Die Daten bleiben während eines Ausfalls des Komponentenverzeichnisses für einen konfigurierbaren Zeitraum gültig.

Bild 8 zeigt dasselbe Komponentenverzeichnis „A“, das jetzt in einem größeren System mit zwei anderen Teilsystemen enthalten ist, d. h. den Komponentenverzeichnissen: „B“ und „C“.

- Jedes Komponentenverzeichnis-Paar synchronisiert bidirektional, d. h. jedes Verzeichnis fordert das andere Verzeichnis für den Inhalt seines Teilsystem-Verzeichnisses an.
- Ein in „A“ registrierter Endpunkt (oder Vermittler) empfängt jetzt den gesamten Inhalt des Systemverzeichnisses („A“ + „B“ + „C“) bei der Synchronisierung mit seinem Home-Komponentenverzeichnis.
- Eine in „B“ oder „C“ registrierte Komponente synchronisiert sich mit dem Komponentenverzeichnis „A“, wenn ihr Home-Komponentenverzeichnis ausfällt. Umgekehrt kann eine in „A“ eingetragene Komponente mit einem anderen Komponentenverzeichnis synchronisiert werden (ein solcher Fluss wird in Bild 8 nicht dargestellt).

[2] Dies ist eine Entscheidung der Systemführung.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

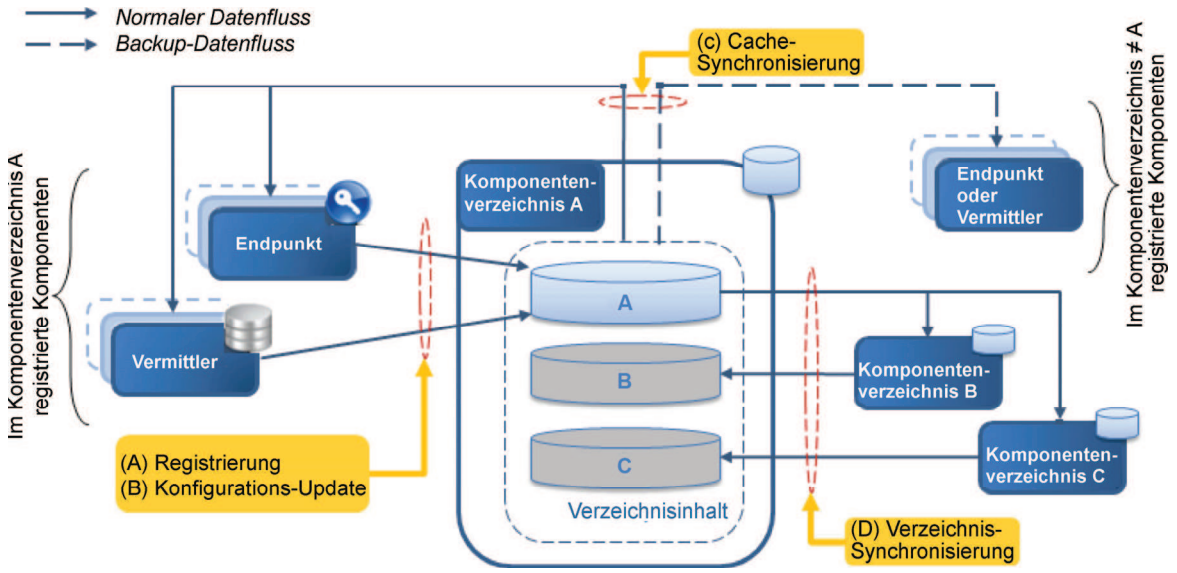

Bild 8 – Datenflüsse mit mehreren Komponentenverzeichnissen

ANMERKUNG Die lokale Cache-Speicherung des gesamten Verzeichnisinhalts ist der Hauptpunkt für ein nichtkritisches Komponentenverzeichnis im System. Die zugrundeliegende Gestaltungsannahme ist, dass Konfigurationsdaten selbst bei einem aus mehreren hundert Komponenten bestehenden System klein bleiben und sich nicht häufig ändern.

Alle in einem Komponentenverzeichnis angezeigten Dienste sind durch Verwendung des https-Protokolls zugänglich, wie in Bild 9 gezeigt.

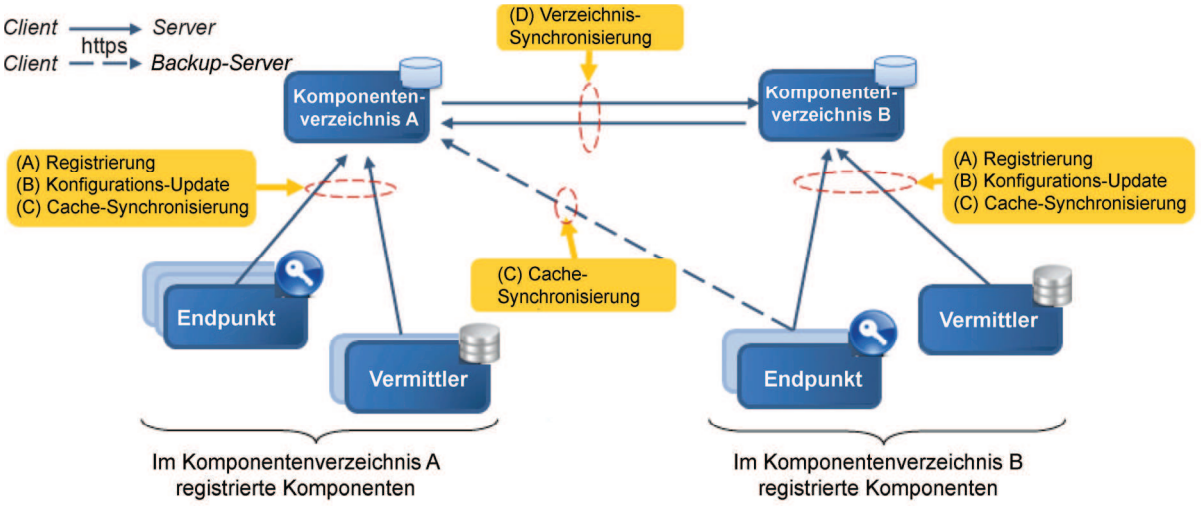

Bild 9 – Dienste und Protokolle des Komponentenverzeichnisses

4.4.4 Von den Komponenten angezeigte Schnittstellen

Bild 10 zeigt die Schnittstellen, die die Spezifikation in Abschnitt 5 festlegt und die von einer konformen Komponente implementiert, d. h. verwendet und angezeigt werden.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

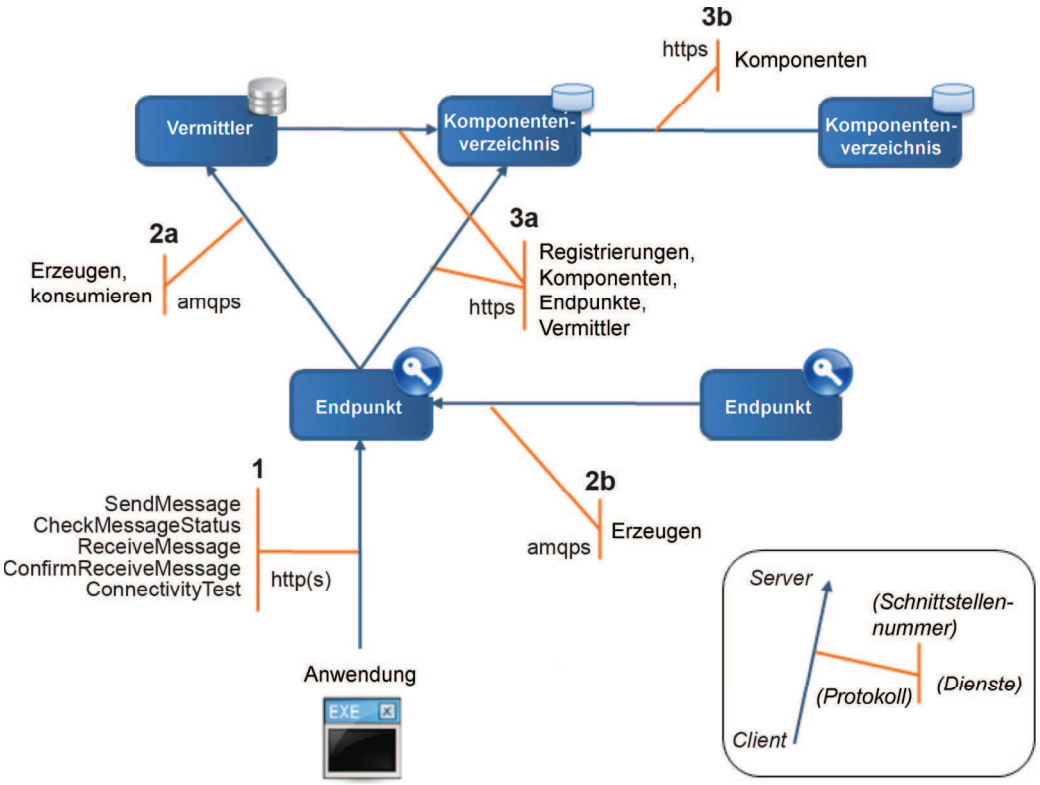

Bild 10 – MADES-Schnittstellen, Dienste und Protokolle

(1) Endpunkt-Schnittstelle für Anwendungen, die HTTP(S) SOAP-Webservice nutzen – siehe 11.1.

- Eine Anwendung sendet eine Nachricht (*SendMessage*) durch das System oder fordert den Zustellstatus einer zuvor gesendeten Nachricht an (*CheckMessageStatus*).
- Eine Anwendung fordert den Download einer empfangenen Nachricht an (*ReceiveMessage*) und bestätigt dem System anschließend, dass es die Nachricht sicher gespeichert oder verarbeitet hat (*ConfirmReceiveMessage*).

  ANMERKUNG Die sichere Speicherung ist in 5.9 definiert.

- Eine Anwendung fordert das System auf, eine Prüfnachricht an eine Peer-Partei zu senden (*ConnectivityTest*), um zu prüfen, ob die Kommunikation mit dieser Partei für einen gegebenen Nachrichtentyp korrekt funktioniert.

(2a) Vermittler-Schnittstelle für Endpunkte, die AMQP verwenden – siehe 6.3.

- AMQP ist ein Protokoll für die Interoperabilität zwischen verschiedener Messaging-Middleware: Es beschreibt keine Schnittstelle, sondern die Bytefluss-Struktur (*Frames*) für den Austausch zwischen zwei TCP-Peers (*in der Leitung*).
- Ein MADES-Vermittler ist ein Server, der Warteschlangen (interner) Nachrichten verwaltet, bis der vorgesehene Empfänger sie empfängt.
- Nach erfolgreicher Authentifizierung durch den Vermittler fungiert ein Endpunkt als Nachrichtenerzeuger für die Versendung einer Nachricht (Erzeugen bzw. *Produce*) und als Nachrichtenverbraucher für den Empfang seiner vorgesehenen Nachrichten (konsumieren bzw. *Consume*).

(2b) Endpunkt-Schnittstelle für andere Endpunkte, die AMQP verwenden – siehe 6.3.

- Die Schnittstelle für die direkte Übertragung zwischen Endpunkten ist dieselbe wie (2a) ohne den *Consume*-Dienst. Ein Endpunkt enthält keine Warteschlangen, in denen andere Endpunkte Nachrichten verbrauchen können.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

(3a) Von Endpunkten und Vermittlern verwendete Komponentenverzeichnis-Schnittstelle – siehe 7.5.

- Die Endpunkte und Vermittler verwenden die Schnittstelle, um sich mit ihrem Home-Komponentenverzeichnis einzutragen, in das sie Konfigurationsdaten per Push-Nachrichten eintragen. Darüber hinaus nutzen sie die Schnittstelle, um eine lokale Kopie des Systemverzeichnisses laufend zu aktualisieren.
- Die Schnittstelle nutzt die REST-Grundsätze. Abfragen und Antworten nutzen das XML-Format und werden anhand von XML-Schemata festgelegt.
- Eine authentifizierte Komponente kann auf die folgenden Ressourcen zugreifen:
  - *Registrierungen*: Abfrage auf Eintritt in das System, um die Zertifikate zu erhalten und zu erneuern.
  - *Komponenten*: Erhalt von Verzeichnisinformationen über alle in dem System registrierten Komponenten, um eine lokale Kopie des Verzeichnisses zu pflegen. Die Antwort enthält entweder den kompletten Verzeichnisinhalt oder nichts, wenn das lokale Verzeichnis bereits aktuell ist.
  - *Endpunkte* (oder *Vermittler*): um Konfigurationsdaten zu einem Endpunkt (oder einem Vermittler) zu erhalten oder solche Informationen zu ändern. Nur eine Komponente kann ihre eigenen Konfigurationsdaten ändern.

(3b) Von anderen Komponentenverzeichnissen verwendete Komponentenverzeichnis-Schnittstelle – siehe 7.5.

- Ein Komponentenverzeichnis verwendet die Schnittstelle, um sich mit einem anderen Komponentenverzeichnis des Systems zu synchronisieren.
- Für die Synchronisierung fordert ein Komponentenverzeichnis „A“ die *Komponenten*-Ressourcen eines Komponentenverzeichnisses „B“ genauso an wie Endpunkte und Vermittler, wenn sie eine Schnittstelle verwenden (3b). Sie fragt jedoch nur den auf die Komponenten des Teilsystems „B“ beschränkten Peer-Verzeichnisinhalt an.

4.4.5 Beispiele für die Architektur von MADES-Systemen

Der Aufbau eines MADES-Systems kann von der aus zwei Endpunkten und einem Komponentenverzeichnis ohne (Bild 11) oder mit Vermittler (Bild 12) bestehenden minimalen Architektur bis hin zu einem Netzwerk aus Endpunkten mit mehreren Vermittlern und Komponentenverzeichnissen (Bild 13, Bild 14) reichen.

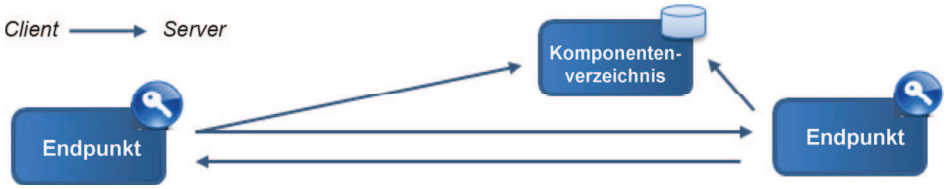

Bild 11 – Minimales MADES-System (ohne Vermittler)

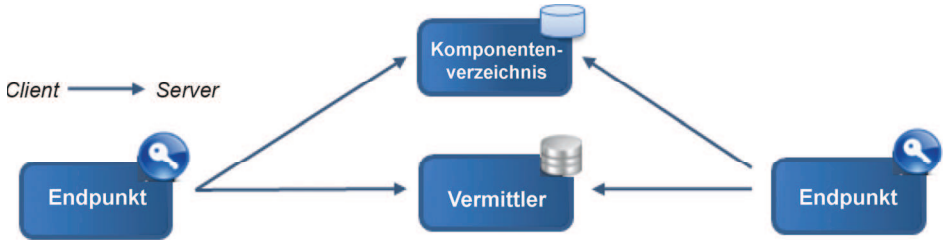

Bild 12 – Minimales MADES-System (mit Vermittler)

Jede der beiden kommunizierenden Parteien, die die Architektur in Bild 12 nutzen, kann entweder den Vermittler oder das Komponentenverzeichnis oder beides beherbergen.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

In einer üblichen Architektur spielt einer der Stakeholder eines Geschäftsprozesses, z. B. „A“, eine zentrale Rolle (Bild 13). Er kann daher einen Vermittler und ein Komponentenverzeichnis beinhalten. Als Hub in der Geschäftsprozess-Logik verfügt er darüber hinaus über einen Endpunkt für den Austausch mit anderen Stakeholdern und ist dafür verantwortlich.

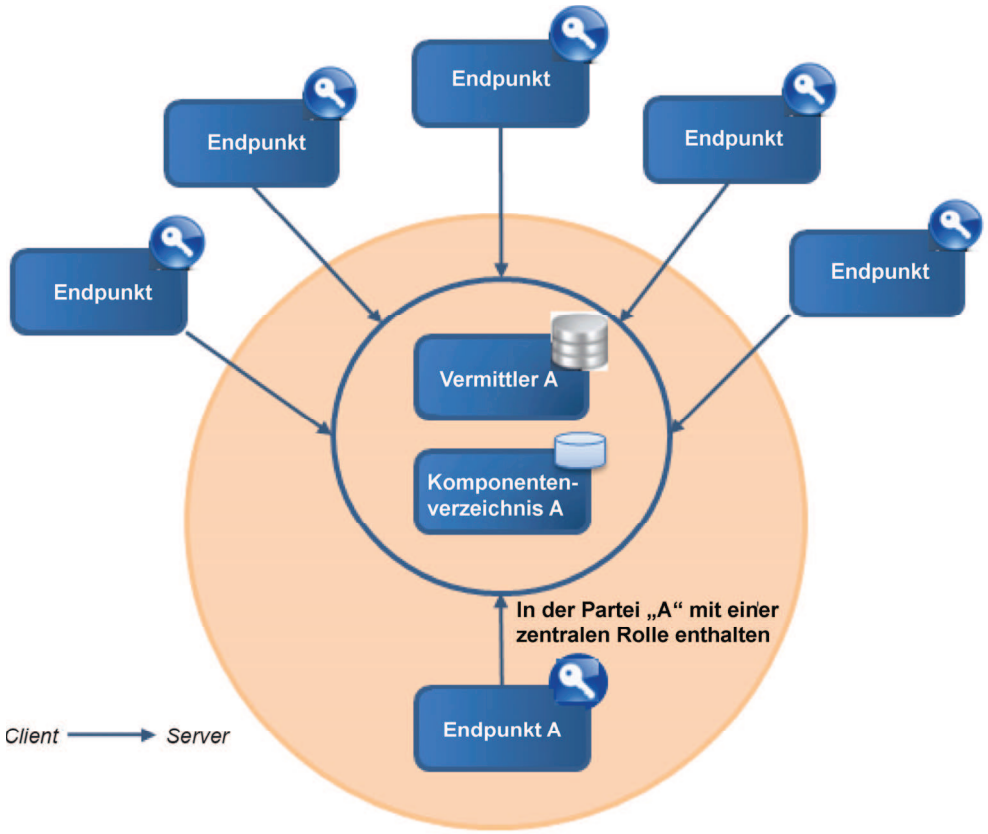

Bild 13 – MADES-System mit einer Partei in einer zentralen Rolle

Ein anderer Geschäftsprozess könnte dieselben oder andere Parteien oder eine Teilgruppe beinhalten, wobei eine Partei, z. B. „B“, jetzt eine zentrale Rolle spielt. Die Parteien können den bestehenden Vermittler „A“ gemeinsam nutzen. Sie können jedoch auch einen anderen und eigenen Vermittler (Vermittler „B“) aus Gründen wie der Hosting-Lokalisierung, der geschäftlichen Kritikalität, des Verantwortungsbereichs, einer abgeschlossenen Dienstgütevereinbarung (SLA, en: service level agreement), Projektplanung usw. verwenden, was zu einer Architektur mit mehreren Vermittlern führt, wie in Bild 14 gezeigt.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

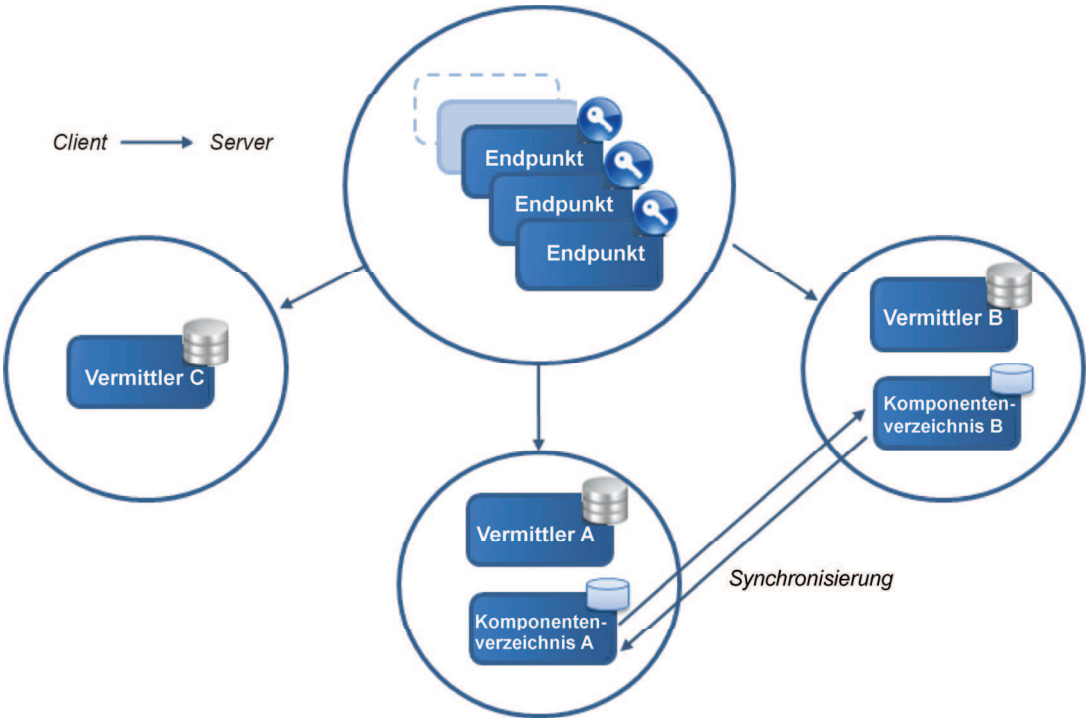

Bild 14 – MADES-System mit mehreren Vermittlern

Bild 14 zeigt zwei Komponentenverzeichnisse, die von zwei Parteien gehalten werden, die die Vermittler A und B besitzen. Es bestehen zwei Komponentenverzeichnisse, möglicherweise aber auch mehr. Die Regeln sind wie folgt:

- Alle Komponentenverzeichnisse synchronisieren sich miteinander.
- Das System hat zwei Komponentenverzeichnisse. Dies wird für den Betriebsfortbestand empfohlen, auch wenn das Komponentenverzeichnis keine kritische Komponente ist und für einige Zeit ausfallen könnte, ohne dass die Nachrichtenzustellfunktion beeinträchtigt würde.

In dem Beispiel in Bild 14 verfügen beide Parteien A und B über ein Komponentenverzeichnis und sind Registrierungsstellen für je ein Teilsystem, d. h. eine Teilgruppe von Endpunkten und Vermittlern des Systems. Die Partei C könnte jedoch ebenfalls ein Komponentenverzeichnis enthalten.

Bild 15 präsentiert dieselbe Architektur aus Sicht einer an jedem Geschäftsprozess beteiligten Partei. Die Partei besitzt einen einzelnen Endpunkt, der in einem eindeutigen Komponentenverzeichnis registriert ist. Hier akzeptiert die Partei direkte Übertragungen und somit eingehende Verbindungen zu dem Endpunkt. Die Architektur kann einige direkte bilaterale Austausche zwischen Parteien ohne direkte Auswirkung auf die Vermittler vorsehen.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

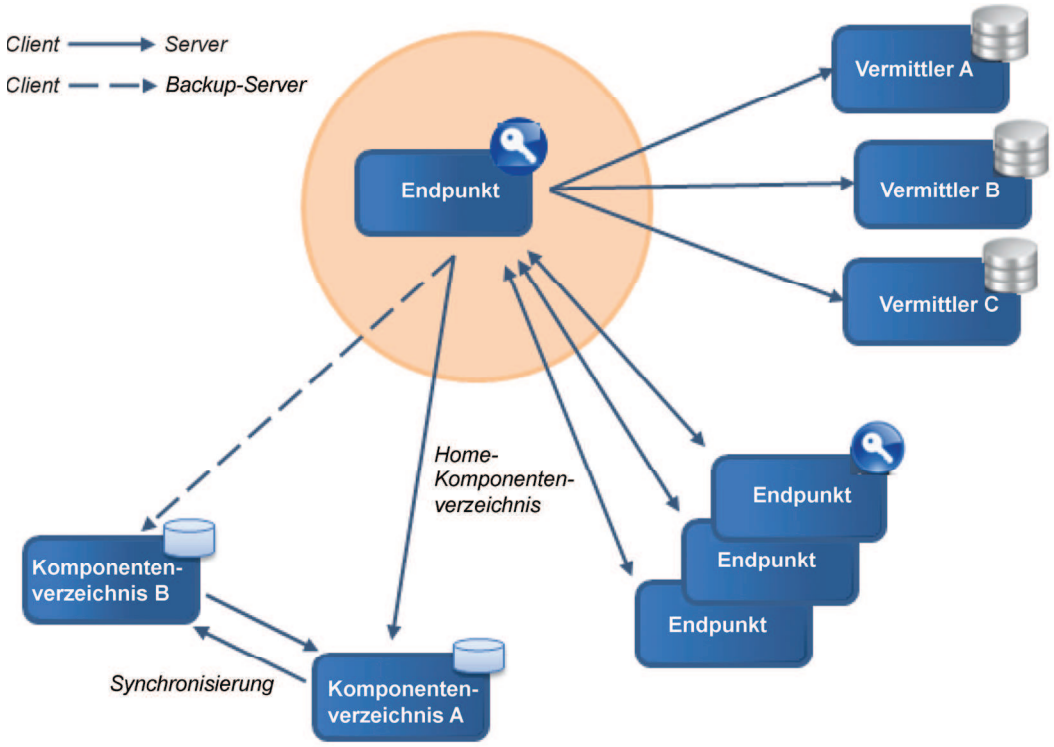

Bild 15 – Verwendung eines einzelnen Endpunkts für mehrere Geschäftsprozesse

Die Partei könnte sich auch entscheiden, mehrere Endpunkte zu enthalten, die jeweils einer Teilgruppe von Geschäftsprozessen oder Nachrichten aus Gründen wie der Hosting-Lokalisierung, der geschäftlichen Kritikalität, der internen Organisation und des Verantwortungsbereichs, der getroffenen Dienstgütevereinbarung (SLA), der Projektplanung usw. zugeordnet sind. Jeder Endpunkt muss dann in einem Komponentenverzeichnis registriert werden und die Endpunkte werden in dem System mit unterschiedlicher ID erscheinen, so als wären sie Eigentum verschiedener Parteien. Solche Endpunkte können nicht in der Master/Slave-Betriebsart funktionieren oder den Lastausgleich des eingehenden Nachrichtenverkehrs in Richtung der Partei übernehmen.[3]

4.5 Sicherheit und Nachrichtenintegrität

4.5.1 Sicherheitsziele und Sicherheitslösung

Die Ziele der MADES-Sicherheit sind:

- Die Sicherheitslösung ist für Anwendungen transparent – eine Anwendung benötigt keine besondere Implementierung, um sicher kommunizieren zu können.
- Alle Kommunikationskanäle sind verschlüsselt.
- Nur der gewünschte Empfänger kann eine Nachricht lesen.
- Der Empfänger einer Nachricht kann den Absender eindeutig identifizieren.
- Unleugbarkeit – Eine Nachricht stellt zusammen mit der dazugehörigen Empfangsbestätigung den eindeutigen Beweis dar, dass der Absender die Nachricht versendet und der Empfänger diese erhalten hat.

Die festgelegte Sicherheitslösung entspricht der X.509 öffentlichen Schlüssel-Infrastruktur (PKI, en: public key infrastructure) unter Verwendung von Zertifikaten und umfasst zwei Sicherheitsstufen: eine Sicherheit der Transportschicht (en: transport layer security) und eine Sicherheit der Nachrichtenschicht (en: message-lever security).

[3] Die hohe Verfügbarkeit eines Endpunkts ist eine Frage der Endpunktgestaltung.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09

- In der Transportschicht verwenden zwei beliebige Komponenten einen verschlüsselten Kanal für die Kommunikation. Darüber hinaus authentifizieren sich beide Komponenten zunächst eindeutig und überprüfen, dass sie gültig registrierte Komponenten des Systems sind, bevor sie Daten austauschen.
- In der Nachrichtenschicht wird jede Nachricht zuerst signiert und dann verschlüsselt.

Jede Komponente verfügt über ein Authentifizierungszertifikat, das für die Sicherheit der Transportschicht (transport layer security) verwendet wird. Jeder Endpunkt hat zwei zusätzliche Zertifikate, die für die Sicherheit der Nachrichtenschicht verwendet werden – eines für das Signieren der versendeten Nachrichten und eines für die Entschlüsselung der empfangenen Nachrichten.

4.5.2 Sicherheit der Transportschicht

Die Sicherheit von zwischen zwei Komponenten ausgetauschten Daten hängt in erster Linie von der Transportprotokollschicht ab. Bei der Kommunikation verwenden zwei Komponenten die „Sicherheit der Transportschicht“ (TLS) für die Verschlüsselung des Kommunikationskanals. HTTPS (oder AMQPS) ist die TLS-gesicherte Version des HTTP (oder AMQP).

Alle kommunizierenden Peer-Komponenten authentifizieren sich gegenseitig mit X.509-Zertifikaten, wie in Bild 16 gezeigt.

Bild 16 – MADES-Transportsicherheit

Die Kommunikation, d. h. die IP-Verbindung, wird immer vom Client initiiert. Bild 10 zeigt alle möglichen Peer-Komponenten.

Dies ermöglicht eine hochsichere Architektur, wenn der Endpunkt nur als Client fungiert, und eine zusätzliche Firewall kann den Schutz durch das Blockieren aller eingehenden Verbindungen erhöhen, wie in Bild 17 gezeigt.

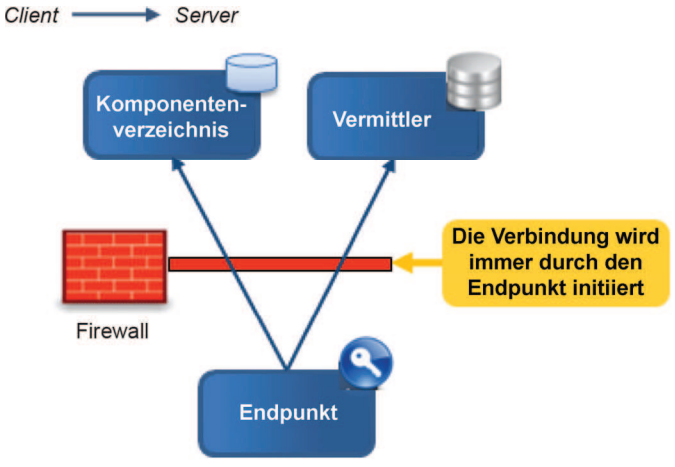

Bild 17 – Sicherheit: geschützter Endpunkt

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62325-503:2021-09