European E-invoicing Service Providers Association (EESPA)

Companion to the Model Interoperability Agreement

Version 4.0

for the Transmission and Processing of Electronic Invoices

and other Business Documents

EESPA acknowledges that the original source material for this document is the Draft Model Interoperability Agreement for the Transmission and Processing of Electronic Invoices and other Business Documents as prepared by the CEN Workshop on Electronic Invoicing Phase 3 and which following finalization in February 2012 was released by CEN. This document has been based on the CEN Workshop Agreement version 0.91 dated 3rd December 2011. It has been substantially amended for use by the service provider community in the light of evolving legal, technical and market requirements.

This Model Interoperability Agreement and its Companion (described below as the MIA/Companion) are available for the use of EESPA Members and are also placed in the public domain for the information of stakeholders and for adoption by other service providers or communities of service providers, which wish to inter-operate with each other. It is recommended that for those service provider organizations that meet the criteria for Membership of EESPA, they seek such status in order to gain the benefit of the community approach. Interoperating service providers are free to use the MIA/Companion in whole or in respect of relevant parts provided that they respect their principles and intent. Any party using the MIA/Companion or any parts thereof does so at its own risk and responsibility.

EESPA AISBL
Avenue Louise 149/24; B-1050 Brussels
Registration number: 0840 293 380

EESPA Secretariat
Dora Cresens
Tiensestraat 12; B-3320 HOEGAARDEN
Tel: +32 475 85 40 39;
dora.cresens@eespa.eu

CONTENTS

Section A Introduction

This Companion document has been prepared by EESPA on behalf of its members and is to be used to support members in adopting and completing the EESPA Model Interoperability Agreement (MIA), between two Parties, being service providers acting for their respective customers. The DoS forms an integral part of the MIA.

The contents of this document do not form any part of the agreement itself and are solely intended to provide guidance and information to support the preparation of an MIA and its attached Description of Services (DoS).

The Companion is divided into five sections:

SECTION A	Introduction
SECTION B	Guidance on completing the Body of the MIA including legal explanations, and the paragraphs requiring selection of options or completion of open elements
SECTION C	Description of a Default Set of Requirements adopted by EESPA to be used in the event of the Parties wishing to deploy a ready-made interoperability solution in which the Transport Protocol and Mode are pre-defined
SECTION D	Guidance for completion of the Description of Services on a Part by Part basis and describing a number of options and model content for each element
SECTION E	Appendices providing detailed information on specific topics

SECTION D adopts the same layout as the DoS, which is used to define the specific technical and operational details of the interoperability agreement between the two Parties. Parties are free to vary and substitute for the recommended default wordings on a case by case basis in agreement with the other Party.

This version 4.0 of the DoS corresponds to Version 4.0 of the MIA. Version control will be applied to always align the MIA version and the Companion. The Companion will be evolved in the light of experience and user expectations. As standards and market practices develop, the Companion will be upgraded.

Section B Guidance on completing the body of the MIA

The MIA consists of the Body of the agreement and its attached free format DoS. This section addresses itself to the completion of the Body of the Agreement.

The MIA is intended to remain a stable document and subject to change in the light of legal changes and user experience. This Section B consists of a series of explanations and guidance as to choices available in the draft MIA and is based on a Chapter and Paragraph commentary based on the numbering sequence of the MIA. There are a number of decisions which the two Parties to an MIA will need to agree, most importantly (but not exclusively) being:

- Section 15 on Liability
- Section 21 on Governing Law and Settlement of Disputes

Whilst Parties are free to vary the terms of the MIA, this is discouraged as numerous and significant changes will over time undermine the benefits of using an industry agreed text. It is preferable that EESPA Members draw attention to commonly experienced issues to the Membership at large through the EESPA Secretariat.

The following are the current sections where guidance is provided:

Section 1 - Parties

The VAT registration number of each Party must be included as it is a requirement of Belgium law.

Section 13.1 – Confidential Information

Part of this section states:

> "Either Party may also disclose to its Customers technical and operational information relating to the other Party's provision of the Interoperability Service, as far as necessary for the performance of this Agreement, with the prior written consent of the other Party (not to be unreasonably withheld or delayed)."

The Parties should consider setting out in the Description of Services technical and operational information that can be disclosed without consent. This will limit the number of times consent will need to be sought.

Section 13.4 – Damages for Breach

Part of this section states:

> "Both Parties agree that the Party affected by a breach of the provisions of this section 13, shall be entitled, without prior notice to the other Party, to appeal to the Brussels' competent court in summary proceedings ("*kort geding procedure*" or "*procédure en référé*") for an order restraining any further unauthorized disclosure or for any such relief the affected Party deems appropriate."

If the Parties have agreed a governing law and/or jurisdiction other than Belgium law and jurisdiction then the "summary proceedings" will need to be amended to reflect the agreed law and jurisdiction.

Section 15 Liability

Parties should always review sections 15.5 (Indirect Damages) and 15.6 (General Liability Limitation) because there are a number of alternative provisions in these sections which will need to be either included or deleted for the final form Agreement.

The Agreement has been drafted in accordance with Belgium law. If the Parties have agreed a governing law other than Belgium law then this whole section needs to be reviewed in particular sections 15.5 (Indirect Damages) and 15.6 (General Liability Limitation).

Section 15.5 (Indirect Damages)

The first part of this section (sections 15.5.1 and 15.5.2) sets out the indirect damages for which neither party will be liable. The second part of the section states that the exclusions of liability in section 15.5 will not apply to any losses and/or damages arising from the items listed in (a) – (e) or do not exclude liability for the items listed in (f) – [(h)].

The Agreement has been drafted to comply with Belgium law and to provide a number of alternatives to the Parties as set out below and the Parties must agree on which to include or not.

Alternative 1

> *"*(g) [direct] damages incurred by a Customer of a Party [(excluding damages of that Customer falling within the categories stated in section 15.5.1 and 15.5.2)] as a result of a breach by the other Party of its obligations under section 13 (Confidentiality) and/or section 12.2 (Responsibility for Security Procedures) for which it is liable in accordance with the terms of this Agreement which involves Customer Confidential Information of that Customer[;]"

If the Parties agree that the indirect damage exclusion of section 15.5 will exclude **all** Customer damages arising from a breach of confidentiality obligations then they should **delete** this section (g). If **not**, then the Parties should **include** this section (g).

However, if the Parties include this section (g) the Parties must also make it clear whether **indirect** Customer damages are to be excluded.

If the Parties agree that indirect Customer damages **are to be excluded** (so a Party would be liable for only direct loss/damages of a Customer arising from a breach of confidentiality obligations) then the wording in square brackets should be **included**.

If the Parties agree that indirect Customer damages are **not** to be excluded (so a Party would be liable for both direct and indirect losses/damages of a Customer arising from a breach of confidentiality obligations) then the wording in square brackets should be **deleted**.

Alternative 2

> "(h) direct damages incurred by a Customer of a Party (excluding damages of that Customer falling within the categories stated in section 15.5.1 and 15.5.2) as a result of a breach by the other Party of its obligations under this Agreement for which it is liable in accordance with the terms of this Agreement."

If the Parties agree that the indirect damage exclusion of section 15.5 should exclude other types of direct Customer damages/losses then this section (h) should be **deleted**.

If the Parties agree that **direct** Customer damages/losses should **not** be excluded then this section (h) should be **included**.

Rather than allow direct damages of Customer to be included in relation to **all** breaches of the Agreement for which it is liable, the Parties are also able **limit** this to allow for direct damages of Customer to be included in relation to a breach of particular sections of the Agreement **only**, for example sections 8.1 and/or 8.2 (Responsibilities in relation to E-Invoices). If the Parties choose to limit to particular sections then they will need to list these as part of this section (h).

Section 15.6 (General Liability Limitation)

The total annual liability of each party to the other is limited to €50,000 and this section 15.6 sets out the circumstances in which this cap will not apply. The Agreement has been drafted to provide a number of alternatives to the Parties. The Parties must therefore choose whether they wish the cap to apply to losses arising from the certain circumstances set out below.

> "(c) any breach of section 13 (Confidentiality) which involves Party Confidential Information;
>
> (d) any breach of section 13 (Confidentiality) which involves Customer Confidential Information;
>
> (e) IPR indemnification under section 15.1;
>
> (f) fines made against a Party by a Regulator as a result of a breach by the other Party of its data protection obligations set out in sections 12 and/or 14 of this Agreement;
>
> (g) costs incurred by a Party as a result of data subject notifications or monitoring required as a result of a breach by the other Party of its data protection obligations set out in sections 12 and/or 14 of this Agreement."

If the Parties agree that the cap **will** apply to any of these, then they must **delete** that section from the Agreement.

If the Parties agree that the cap **will not** apply to any of these then they must **include** the wording of that section in the Agreement.

Section 19.1 – Assignment

This section states:

> "Neither Party is entitled to assign or transfer the Agreement or any of its rights, liabilities or obligations under the Agreement without the prior, written consent of the other Party. However, either Party may assign this Agreement without the consent of the other Party to a successor by merger or acquisition of all or substantially all of its assets provided that the other Party is given prior written notice."

Under Belgium law the benefits and burdens under this Agreement and all of its provisions will automatically follow the related assets in case of a transfer, whereby a notice can be given. This is not the case under other legal systems (such as UK law) so if a different governing law is agreed by the parties this provision will need to be reviewed.

Section 20.3.1(d) – Termination on Certain Events

This section states:

> "20.3.1 Either Party may terminate the Agreement immediately by written notice if the other Party:
>
> d) fails to meet any provision of a service level agreement set out in the Description of Services entitling that Party to terminate this Agreement."

If the parties intend for this section to be applicable then the parties must set out a service level agreement within the Description of Services with specific triggers that entitle a party to terminate this Agreement. For example service levels that relate to availability with a trigger entitling termination such as failure to meet the availability SLA in a period of at least 3 consecutive months in any 12 month period entitles a party to terminate in accordance with section 20.3.1(d).

Section 20.3.2 – Termination on Certain Events

> "20.3.2 This Agreement will automatically terminate when a Party is declared bankrupt."

Under BE law, in the case of bankruptcy of a Party, the agreement will continue with the curator or, when explicitly so foreseen in the contract, it will automatically end on the bankruptcy declaration. This is not always the case under other legal systems so if a different governing law is agreed by the parties this provision will need to be reviewed.

Section 21.1 – Governing Law

This section states:

> "Without prejudice to any mandatory national law which may apply to the Parties regarding recording and storage of E-Invoices and Electronic Business Documents or confidentiality and protection of personal data, the Agreement is governed by the laws of Belgium unless any other country is agreed between the Parties and specified within Part 8 of the Description of Services (Other Specified Terms and Conditions)."

The Agreement is subject to Belgium law. However, the Parties are able to agree a different governing law and specify this in the Description of Services. The Parties will need to review the entire Agreement and make any other changes required as a result of the change in governing law.

Section 21.2 – Dispute Resolution

Part of this section states:

> "This provision does not prejudice either Party's right to have urgent litigation cases under this Agreement discussed in summary proceedings ("kort geding procedure" or "procédure en référé") before the Brussels' court in Belgium."

If the Parties have agreed a governing law and/or jurisdiction other than Belgium law and jurisdiction then the "summary proceedings" will need to be amended to reflect the agreed law and jurisdiction.

The second part of this section requires the Parties to agree on how disputes relating to the Agreement will be resolved. Parties should choose "Alternative 1" if they wish disputes to be resolved by arbitration or "Alternative 2" if they wish disputes to be resolved by the courts.

If the parties choose "Alternative 1" (disputes to be resolved by arbitration) then each Party will still have the right to have urgent litigation cases under this Agreement discussed in summary proceedings. If the Parties have agreed a governing law other than Belgium then the following part of section 21.2.2 will need to be reviewed and amended.

> "The present arbitration section does not prejudice either Party's right to have urgent litigation cases under this Agreement discussed in summary proceedings ("kort geding procedure" or "procédure en référé") before the Brussels' court in Belgium."

If the parties choose "Alternative 2" (disputes to be resolved by the courts) then the Belgium courts have sole jurisdiction. If the parties have agreed a governing law other than Belgium then the parties should also review this section and amend the courts which will have jurisdiction.

Section 22.8 – Compliance with competition and similar laws

As the Agreement will be between competitors, this section is required under Belgium law.

Section C Default set of requirements

EESPA has established a DEFAULT Set of Requirements adopted by EESPA to be used in the event of the Parties wishing to deploy a ready-made interoperability solution for E-Invoices, in which the Transport Protocol and Mode are pre-defined. It is recommended for use where possible so that the time and cost associated with establishing interconnections can be minimised. It is designed to be immediately useable.

The DEFAULT Set of Requirements represents a single option with all elements MANDATED.

To ensure clarity, the DEFAULT Set of Requirements can only be described as such where no Mandated elements have been changed.

The MANDATORY elements within the DEFAULT Set of Requirements are:

Relevant to Part 3 of the DoS: Transport Protocol

Transport protocol	AS2 (Which will provide the technical acknowledgement of delivery)
Envelope	The GS1 Standard Business Document Header (SBDH), as defined within Appendix 3 of this Companion
Addressing/Routing	Bilateral exchange of addressing and routing information pending the agreement and deployment of an EESPA scheme for Addressing & Routing.

Relevant to Part 4.1 of the DoS: Mode and Format Standard

Format Standard	UBL (CEN BII) with fields mapped in accordance with the relevant section within this Companion
Invoice	Structured XML Data File plus a signed PDF
Signature	Qualified Digital Signature embedded within the PDF and signed by the Sending Party or the Sender. The Sending Party is responsible for ensuring that the PDF is signed and that a validation is provided to the Receiving Party if agreed under the terms of Chapter 9.2 of the MIA.
Conformance	The Sending Party guarantees that each mandatory invoice field is identical in the PDF and in the dataset *as this was created by the Sending Party*.
Business acknowledgement	Not mandatory in this version ... planned for review within EESPA and future inclusion within the Default.

Further detailed guidance is provided in the sections that follow, in particular, within Section D.

Section D Completing the Description of Services of the MIA

Introduction

SECTION D adopts the same layout as the DoS, which is used to define the specific technical and operational details of the interoperability agreement between the two Parties. Parties are free to vary and substitute for the recommended default wordings on a case by case basis in agreement with the other Party.

Any variation or Amendment of the Description of Service must be carried out in accordance with the terms set out Paragraph 5.3 and 19.2 of the MIA.

The following provides a summary of the Parts making up the Description of Services:

Part 1: Parties and Contact Information

This section of the Description of Services includes information about the Parties to the Interoperability Agreement and should be completed separately by each Party including Legal, Technical and Support contacts.

Part 2: Scope of Agreement

Within this free-format section, details can be included, as required, to cover general details agreed by the Parties that set boundaries to the Agreement. These could include, but are not limited to: which documents types are included; whether it is a uni-directional or bi-directional Agreement for each document type; which territories are covered; are customers to be defined in any way, and any other elements relevant to scope

Part 3: Transport Protocol

Within this free-format section, details MUST be included to cover details agreed by the Parties that define the Transport Protocol to be adopted in support of the Interoperability Service. These would include, but are not limited to the choice of network, transport protocol itself, message envelope or container, file restrictions, any additional message features and technical delivery acknowledgements.

Part 4.1: E-Invoice Message Payload: Mode and Format Standard

Within this free-format section, details MUST be included to cover details agreed by the Parties that define the Mode-specific details for achieving compliance, authenticity, integrity and legibility within the Interoperability Service. These form the basis of the way in which the Parties will support their customers in meeting legal and compliance requirements as well as fulfilling operational expectations in relation to e-invoices and electronic business documents. This include, but are not limited to the agreed Format Standard, the selected Mode (as defined), agreed validations, checks and controls, and business level acknowledgements including rejections.

Part 4.2: Other Electronic Business Documents in Message Payload

Within this free-format section, details can be included to cover general details agreed by the Parties that define the Interoperability Services relating to documents other than Invoices (which are covered specifically within Part 4.1).

Part 5: Set-Up and Service Procedures

Within this free-format section, details can be included, as required, to define the timing and nature of specific activities to be undertaken by each Party in setting up and maintaining the Interoperability Service. These could include, but are not limited to: a project timetable for establishing the Interoperability Service; Testing and sign-off processes; Use of Test Services prior to live exchange; Activity reporting; Maintenance planning for events that could affect the Interoperability Service; Error reporting; etc.

Part 6: Charges

Within this free-format section, details can be included, as required, to define any charges that will apply between the Parties relating to the provision of the Interoperability Service. As indicated in the MIA, each Party shall freely and independently determine its Customer charges and shall be responsible for collecting Customer charges from its own Customers. This section is to allow charges for establishing or maintaining the Interoperability Service that have been negotiated and agreed between the Parties to be described so that they form a part of the MIA.

Part 7: Certification of Internal Controls

Within this free-format section, details may be included, if required, to define ways in which each Party agrees to provide to the other Party evidence of any Certification of its internal controls (Certification).

Part 8: Other Specified Terms and Conditions

Within this free-format section, details may be included, if required, to define any additional terms or conditions that both Parties agree to include within the MIA, including any Service Level Agreements and any additional indemnity or warranties.

Completing Part 1: Parties and Contact Information

Noting that the Parties are also identified at a corporate level within the initial section of the MIA, Part 1 is specifically to share a contact within each company who will be responsible for the legal and technical engagement resulting from this Agreement. Details should be completed in full and any subsequent changes amended and recorded so that the contact details available to both Parties remains up to date.

The legal contact point should be responsible for notices and dispute resolution as set out in Paragraph 21.2 and 22.4 of the MIA.

As set out in Paragraph 7.8 of the MIA all relevant contacts relative to technical, commercial and other matters including Support should be clearly set of this section of the DoS.

Part 1. Parties and Contact Information	
Party A.	**Party B.**
Service Provider Name:	Service Provider Name:
Contact(s) for Legal Notices:	**Contact(s) for Legal Notices:**
Contact Person:	Contact Person:
Address:	Address:
Email:	Email:
Phone:	Phone:
Technical Contact(s):	**Technical Contact(s):**
Contact Person:	Contact Person:
Address:	Address:
Email:	Email:
Phone:	Phone:
Support Contact(s):	**Support Contact(s):**
Contact Person:	Contact Person:
Address:	Address:
Email:	Email:
Phone:	Phone:
Commercial Contact(s):	**Commercial Contact(s):**
Contact Person:	Contact Person:
Address:	Address:
Email:	Email:
Phone:	Phone:

Completing Part 2: Scope of Agreement

This is a free format section to allow the Parties to set out and agree upon any aspects of the Interoperability Services which have a definable scope. Although it is a free format section, it is required to include details sufficient to describe the scope clearly. As required in paragraph 3.1 of the MIA, this section should be used to defined E-invoices and/or Electronic Business Documents to be exchanged and such other services as might be mutually agreed. This and the other sections of the DoS should satisfy the requirement set out in paragraph 4.1 and 4.2 of the MIA to describe the specific Interoperability Service to be provided by the Parties to each other.

The samples included in the table here are considered to be the minimum that should be included within this Part 2 of the DoS.

Part 2. Scope of Agreement
1. The document types covered under this Agreement are those listed below: a) Invoices b) Credit Notes
2. The exchange of documents as covered under this Agreement is to be bi-directional such that documents can be exchanged with either Party acting as the Sending Party or Receiving Party or is to be unidirectional with one Party acting as the Sending Party and the other as Receiving Party
3. The exchange of documents covered under this Agreement can be for Invoices or Electronic Business Documents originating from within any of the following territories: a) Any Member State of the European Union b) European Union plus EEA and Switzerland c) The above plus other defined territories
4. The exchange of documents covered under this Agreement can be for documents being received within any of the following territories: a) Any Member state of the European Union b) European Union plus EEA and Switzerland c) The above plus other defined territories
5. (Example 1). The exchange of documents covered under this Agreement can be between any Customers of either Party.
6. (Example 2). The exchange of documents covered under this Agreement can be between any Customers of either Party as agreed by both Parties in advance.
7. Add any additional services such as archiving
8. Add any agreed procedures relative to variation of the DoS in addition to those defined in Paragraph 5.3 of the MIA

Completing Part 3: Transport Protocol

Again, this is a free-format section, but responses at least against the details identified in the table below MUST be included to cover the basic requirements for the Transport Protocol to be adopted in support of the Interoperability Services.

It is important to ensure that in accordance with paragraph 5.2 of the MIA, each Party agrees to receive, transmit, process and route, as applicable, Messages in accordance with procedures set out in Part 3 – Transport Protocol, Part 4 – Message Payload and as described within Appendicex 3, Envelope Standard, Appendix 4 – EESPA Response Messages and Appendix 5 – Addressing and Routing Protocol.

Procedures for the Transmission of the Messages are further defined in paragraph 6 of the MIA.

For quick reference purposes, the following definitions (from within the MIA) are included here for clarification:

Message:

- A single electronic transmission that consists of a header containing addressing and routing information and a payload which includes an E-Invoice or an Electronic Business Document or a Business or Technical Acknowledgement or response Datasets.

Transmission Protocol:

- Means a standard that allows for secure and reliable packaging, routing and transporting of Messages.

Note: Where the Default option is adopted, the Transport Protocol is AS2 (including the Technical Acknowledgement).

Checks and Controls *(See also "Section D - Completing Section 4.1" for further details on Checks and Controls)*

This Transport Protocol Section must define the Checks and Controls relating to the transfer of the Envelope.

This is referred to as "Level 1" Checks and Controls and provides only a Technical Acknowledgement of the exchange and receipt.

The default EESPA acknowledgement is the Message Delivery Notification (MDN) as provided where the AS2 protocol is adopted.

All other Checks and Controls are defined within "Section D - Completing Part 4.1".

NOTE: *The method used to undertake the "Technical Acknowledgement" Checks and Controls and the communication of the outcomes between the Service Providers must be agreed between the Parties and defined within Section 3 of the Description of Services.*

Part 3. Transport Protocol

1. The Network to be used to provide the Transport infrastructure for the Interoperability Services will be the Public Internet (*or perhaps* "The XXXX private Network or VAN operated by XXXX")
2. The Transport Protocol to be adopted across the Network included in point 1 above will be:

   Note: The EESPA Default is AS2.
3. The Message Envelope (Container) will be the"Standard Business Document Header (SBDH)" *(details see appendix 3)*
4. The Maximum File size that can be exchanged, and which may contain multiple Message Envelopes within the file, is _____nMBytes or Unlimited
5. Addressing and Routing: Details of the bilateral exchange of addressing and routing information to be used when sending the Messages to identify the customers: Sender, Receiver, and also the Service Provides: Sending Party and Receiving Party. Reference should be made to the details within Appendix 3 (Envelope Standard) and Appendix 5 (Addressing & Routing Protocol) to ensure the consistent treatment of Addressing and Routing Identifiers.

e.g.	Sender's Addressing ID	VAT Number
	Receiver's Addressing ID	Account Reference
	Sending Party's Routing ID	CEGEDIM
	Receiving Party's Routing ID	TRADEX
6. With reference to Appendix 3 (Envelope Standard) of this Companion, any qualifiers to be used within the Standard Business Document Header (the envelope) must be agreed by the Parties and defined here.

e.g.	Sender's Addressing ID Qualifier	= "VATIN"	(The VAT Number)
	Receiver's Addressing ID Qualifier	= "NONE"	(No Qualifier Provided)
7. Message level signing, encryption and compression
   (example 1) ... is not used
   (example 2) ... is used based on 128 bit encryption
   (example 3) ... is used based on .....
8. Technical Delivery of the Message(s) will be Acknowledged using the default AS2 protocol., as will Technical Rejections
9. Others as agreed by the Parties ....

About AS2

AS2 supports the exchange of business to business transactions by providing an “envelope” for the data, allowing it to be sent, received and acknowledged over the Internet (or another TCP/IP-based network) using the HTTP protocol.

About the Standard Business Document Header (the envelope)

There are several types of envelopes available in the market. Most of them are linked to a single format. The GS1 Standard Business Document Header (SBDH) is independent from the format and permits the transport of structured data and PDF files. Also, the SBDH supports multi party addressing without looking into the structured data and it is well defined and used in practice.

Main benefits of the SBDH:

- One common standard for integration development for all interoperability modes
- Using the section “business scope” the used EESPA interoperability mode can be defined
- One common standard for all formats (EDI and XML)
- Business documents can easily be identified
- Routing information available without parsing the documents
- Well defined

More information on how to use the SBDH can be found in Appendix 3

About the technical acknowledgment (acknowledgments/rejections)

EESPA proposes to use the standard AS2 technical acknowledgement/rejection. For more information see Appendix 4. Where the Transport Protocol agreed between the Parties is a protocol other than AS2 (i.e. where an alternative communication option is adopted by the Parties) then the Parties are recommended to implement an equivalent technical acknowledgement. This could be part of the communication protocol or using the EESPA Response Message (See Appendix 4).

Completing Part 4.1: E-Invoice Message Payload Mode and Format Standard

Section 4.1 of the Description of Services is where details are set out to confirm the Message Payload that will be exchanged between the Parties, including the Mode and Format Standard to be used. These are defined terms set out in paragraph 2.1 of the MIA.

Mode	Means the method chosen by the Parties through which the Sender and Receiver can satisfy their obligations in respect of the authenticity of origin, the integrity of content and the legibility of the E-Invoice under applicable law or regulations in relation to the particular E-Invoice.
Format Standard	Means the standard for the formatting of an Electronic Business Document or Dataset according to pre-defined syntax and/or schema as described in the Description of Services.

The Parties further need to agree and specify, if not already covered in the details below, any additional operational procedures to be followed and the carrying out of such checks and controls as the Parties require. Please see Paragraph 8.1.1 and 8.2 of the MIA. This also covers rejections and where EESPA Response Messages are to be used, they are set out in Appendix 4. **Checks and Controls**

These must be defined using the following three Levels:

Level 1	Transfer Status (Technical Acknowledgement) – Covered within Section D, "Completing Section 3".
Level 2	Status updates, related to SP-SP Processing and which can be automated on receipt of the e-Invoice
	2a. Legal compliance (EU Directive, Country and Industry)_
	2b. Business rules compliance undertaken by the SP for or on behalf of their Customer
Level 3	Status updates, related to invoice processing subsequent to the automated checks undertaken within Level 2 and related to the internal customer workflow process.
	e.g. Customer status updates, such as invoice loaded into ERP or approved for payment.

NOTES:

(1) *The method used to undertake these Checks and Controls and the communication of the outcomes between the Service Providers must be agreed between the Parties. The following sets out one option for this:*

Level 1 Provided using the AS2 acknowledgement protocol

Level 2 Provided by exchanging the EESPA Response Message (See Appendix 4)

Level 3 Could either be provided using the EESPA Response Message or by the exchange of other standard messages, such as APERAK, REMADV, etc.

(2) The communication of the outcomes (of these Checks and Controls) between the Service Providers must be agreed between the Parties.

(2a) Where the EESPA Response Message is used, this will be conveyed as a Business / Technical Acknowledgement within the Message Payload *and as described within "Section D - Completing Section 4.2".*

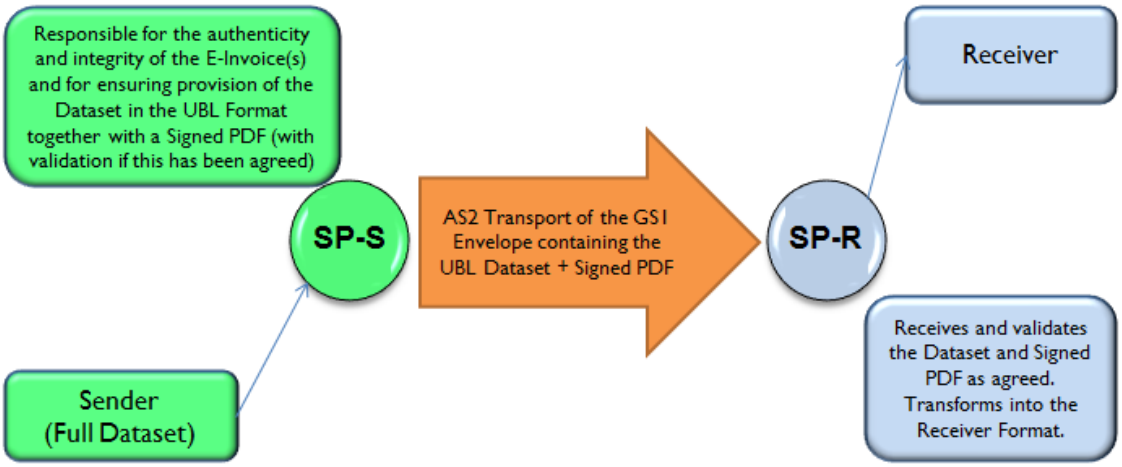
(2b) Where other messages, such as Application Integration Messages (e.g. APERAK), are used to convey the outcomes, this will be conveyed as an "Other Business Document" as described within "Section D - Completing Section 4.3".

This section sets out how Part 4.1 of the Description of Services should be completed for the following EESPA Modes:

Default Mode	Mandated approach to simplify adoption and the anticipated growth of interconnections.
Mode 1a	Digital Signatures on PDF + dataset formatted and attached as a structured file
Mode 1b	Digital signature applied on dataset (with or without a PDF attached)
Mode 2	EDI
Mode 3	Business Controls

Mandatory 4.1 details for Default Mode

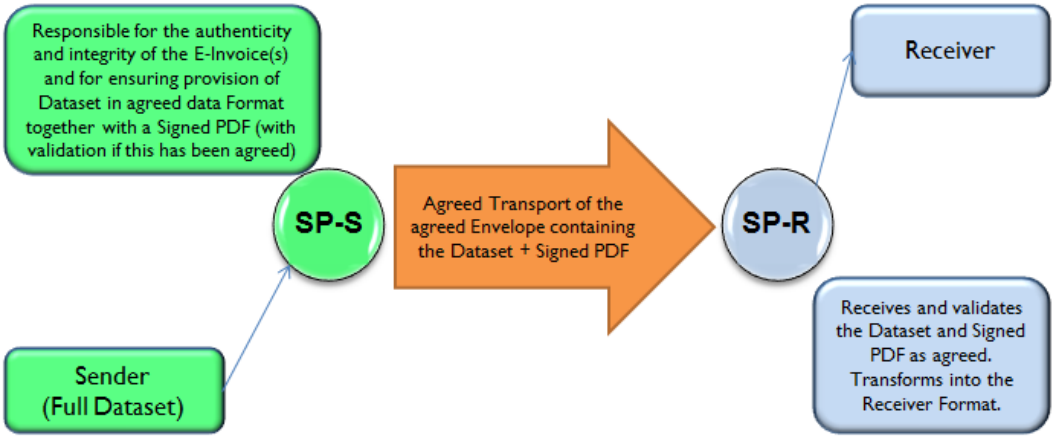
The following information is based on the ”Default Mode” being adopted, as outlined in Section C. Alternative options are noted within this section and set out within Appendix 2.



Part 4.1 E-Invoice Message Payload Mode and Format Standard	
Data Format	UBL (CENBII version 1) and with fields mapped in accordance with the relevant section within the EESPA Companion v3.0.
Data Rules	Mandatory Fields included according to the EU directive 2006/112/EC and mapped in accordance with the relevant section within the EESPA Companion v3.0.
Invoice	Structured UBL (CENBII version 1) Dataset + signed PDF.
Original Invoice	Signed PDF.
Signature	Qualified Digital Signature, embedded within the PDF. The invoice Dataset is not signed
Authenticity of Origin	The Sending Party guarantees the Authenticity of Origin through the existence of a Customer Agreement with each Sender
Integrity of Content	This is demonstrated by the Sending Party being responsible for ensuring that the PDF is signed and that a validation is provided to the Receiving Party if agreed under the terms of Chapter 9.2 of the MIA.
Legibility	Is ensured through the digitally signed PDF Original Invoice
Checks & Controls	Levels 1, 2 and 3 details as described earlier within this section.
Options	Additional Response Messages may be exchanged as agreed by the Parties and listed here. Details of the EESPA Response Message are included within the EESPA Companion v3.0.

MODE 1a: Digital Signatures on PDF + dataset formatted and attached as a structured file

Note: The dataset may be signed (possibly within the PDF signature wrapper) or unsigned



Part 4.1 E-Invoice Message Payload Mode and Format Standard

In this Mode, 1a:

(a) the Sending Party receives a full invoice Dataset from the Sender and is responsible for providing the E-Invoice Dataset and ensuring that the PDF is signed and that a validation is provided to the Receiving Party if agreed under the terms of Chapter 9.2 of the MIA

(b) The PDF is the original invoice.

(c) The Dataset may also be Signed if agreed and defined within this section of the DoS)

1. **E-Invoice creation:**
   - Mandatory Fields presence control: *See Appendix 1*
   - **Optional**: Additional validation (e.g. presence of specified references, such as delivery note number): *<INCLUDE LIST HERE> and indicate action that would be taken where validation fails.*
   - PDF creation is either (a) by the Sender or (b) by Sending Party from the dataset <Indicate which is to be used>
   - Signature validation is either (a) provided by the Sending Party or (b) The responsibility of the Receiving Party / Receiver <Indicate which is to be used>
   - The Sending Party is responsible for ensuring that each mandatory field is correctly mapped to be identical in the both the PDF and in the dataset *where either or both format is created by the Sending Party.*
   - Dataset creation: The format for the dataset to be defined in Payload section below (See also Appendix 2). The dataset can be either a full invoice (i.e. with all the same data elements as are present in the PDF) or a partial invoice (such as just the header and footer information). The dataset as sent to the Receiving Party is created from the Full Invoice dataset as received from the Sender by the Sending Party and must comply with Payload format requirements as described in the Payload format documentation (including mandatory fields presence)
   - Digital signature of the PDF to be made with a compliant certificate: *<INCLUDE DETAILS HERE>*

2. **Payload Component (E-invoice exchanged):**

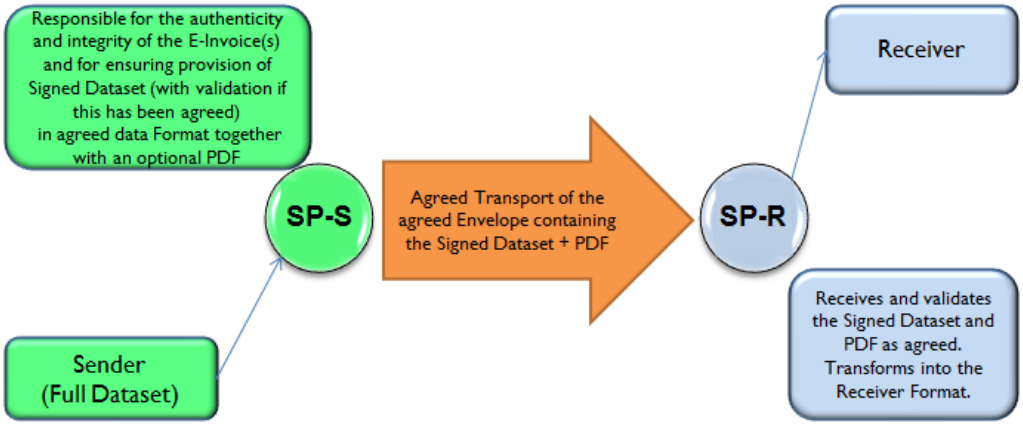
   digitally signed PDF + attached dataset (which may also be signed if agreed and defined within this section of the DoS)

- E-invoice Format: digitally signed PDF + dataset in format agreed and recorded here. See Appendix 2 for default and suggested options.
- Message envelope: *See Appendix 3 for default option*

3. **Authenticity of Origin: The** PDF is digitally signed either by the Sender or by the Sending Party or a partner of the Sending Party, named xxx, on behalf of the Sender. The Sending Party provides for the Authenticity of Origin through the existence of a Customer Agreement and / or an electronic invoicing mandate with each Sender.
4. **Integrity of Content:** is demonstrated by the digital signature on the PDF AND electronic certificate validations as defined within the E-Invoice Creation section above.
5. **Legibility:** is achieved by the digitally-signed PDF.

- **Checks & Controls** Levels 1, 2 and 3 as described earlier within this section.

MODE 1b: digital signature applied on dataset (with or without a PDF attached)



Part 4.1 E-Invoice Message Payload Mode and Format Standard

In this mode, 1b:

(a) The Sending Party receives from the Sender a full invoice dataset and is responsible for providing a PDF version and a Signed E-Invoice Dataset and that a validation is provided to the Receiving Party if agreed under the terms of Chapter 9.2 of the MIA and ensuring that the PDF is signed.

(b) A PDF can be attached to the Structured File dataset.

(c) The PDF can be generated by the Sending Party or directly by the Sender

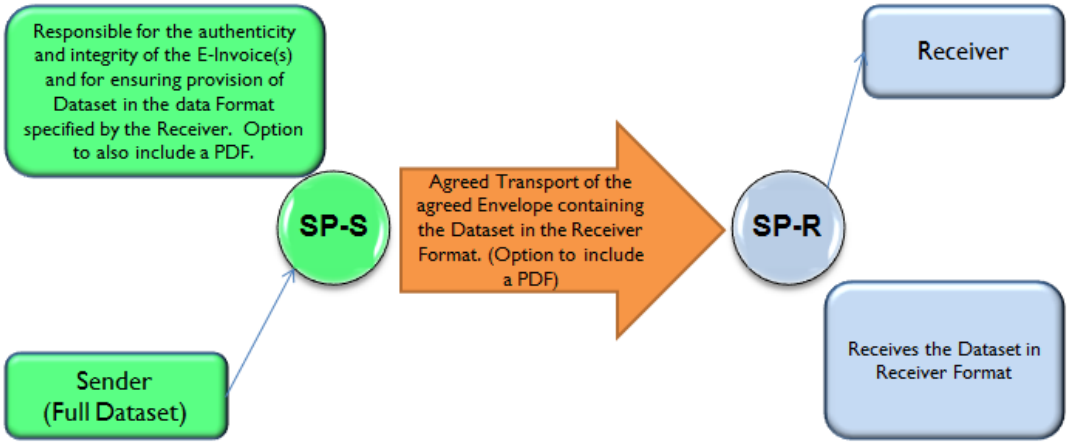
1. (d) The PDF may optionally be signed if agreed and defined within this section of the DoS). **E-Invoice creation**:
   - Mandatory Fields presence control: *See Appendix 1*
   - **Optional**: Additional validation (e.g. presence of specified references, such as delivery note number): *<INCLUDE LIST HERE> and indicate action that would be taken where validation fails.*
   - Structured File generation: format defined in Payload section 2. It is necessary a compliant Invoices with all mandatory fields (including lines).
   - **Optional PDF creation**: Where included this would be created by either (a) the Sending Party or (b) the Sender <Indicate here if a PDF is to be included and by whom this will be created>.
   - The Sending Party is responsible for ensuring that each mandatory field is correctly mapped to be identical in the both the PDF and in the dataset where either or both formats is created by the Sending Party. Digital signing of the Dataset to be made with a compliant certificate: *<INCLUDE DETAILS HERE>*
   - Signature validation is either (a) provided by the Sending Party or (b) the responsibility of the Receiving Party / Receiver <Indicate which is to be used>

2. **Payload Component (E-invoice exchanged):**

   digitally signed dataset + option to attached PDF (The PDF may be signed or unsigned)
   - E-invoice Format: digitally signed dataset with a compliant certificate in format agreed and recorded here. See Appendix 2 for default and suggested options.
   - Message envelope: *See Appendix 3 for default option*

3.	**Authenticity of Origin: The** dataset (structured file) is digitally signed either by the Sender, Sending Party or a partner of the Sending Party, named xxx, on behalf of the Sender. The Sending Party provides for the Authenticity of Origin through the existence of a Customer Agreement and / or an electronic invoicing mandate with each Sender.
4.	**Integrity of Content:** is demonstrated by the digital signature on dataset (structured file) AND electronic certificate validations as defined within the E-Invoice Creation section above.
5.	**Legibility:** is either achieved using the optional PDF *or* has to be performed by each Party (Sending / Receiving) to their respective customers (Sender / Receiver) *u*sing the Invoice Dataset.
6.	**Checks & Controls** Levels 1, 2 and 3 details as described earlier within this section.

MODE 2: EDI



Part 4.1 E-Invoice Message Payload Mode and Format Standard
In this Mode 2, EDI: (a) The Sending Party receives from the Sender a full invoice dataset. (b) The Sending Party creates the E-Invoice on behalf of the Sender in a structured File Format without digital signature meeting requirements set out in 1994/820/EC. (c) **Optional Reference:** The EDI mode could be based on the GS1 certified process adhering to article 289bis (3CA n°136 August 7th, 2003) of the French Tax Code, but is applicable within all other EU member states. **1. E-Invoice creation:** ○ Mandatory field presence control: Mandatory fields are specified by the sending party's local tax authority's legal requirements. (See addendum for EC defined minimum fields) ○ Structured File generation: format defined in Payload section 2.
2. Payload Component (E-invoice exchanged): EDI format adhering to 1994/820/EC. ○ E-invoice Format: dataset (structured file) as agreed. ▪ A recommended format is EDIFACT EANCOM D97V2/V3 format adhering to GS1 France certified compliant EDI e-Invoicing process (http://www.gs1.fr/gs1_fr/layout/set/print/solutions/facture_dematerialisee). However, any other mutually agreed format (EDI based, XML, etc.) between seller and buyer is allowed, as permitted within 1994/820/EC. ○ Message envelope: *See Appendix 3 for default option*
3. Authenticity of Origin: Authenticity of the origin and integrity of the content are guaranteed by a mutual fulfilment of a Partner list (a list of e-Invoicing trading partners for this mode) and Summary list (a journal of the sent or received invoices, with dates and identification of the sender and receiver that preserves the identity of messages sent and received. A well implemented non-signed EDI process can also be interpreted as a compliant business controls method. **T**he Sending Party guarantees to the Receiving Party that the issuer of the E-Invoice is the Sender and that he has all authorization from him to create the e-Invoice on its behalf. This is achieved by the existence of a customer agreement and an electronic invoicing mandate (mandates are only required where local tax authorities explicitly require them).

In addition both Sending and Receiving Parties maintain an individual Partner list of all e-Invoicing trading partners and an audit history of beginning or ending dates of each electronic invoice relationship. While mandatory in France this requirement may not be expected in other EU member states, however EESPA recommends maintaining a partner list as best practice.

The trading partner file must contain the following (immutable) data:

- Name and address of trading partners
- Definition of issuer and/or receiver of invoices
- Date(s) of beginning/end of invoice processing partnership with each trading partner
- A log of changes to any of the above data

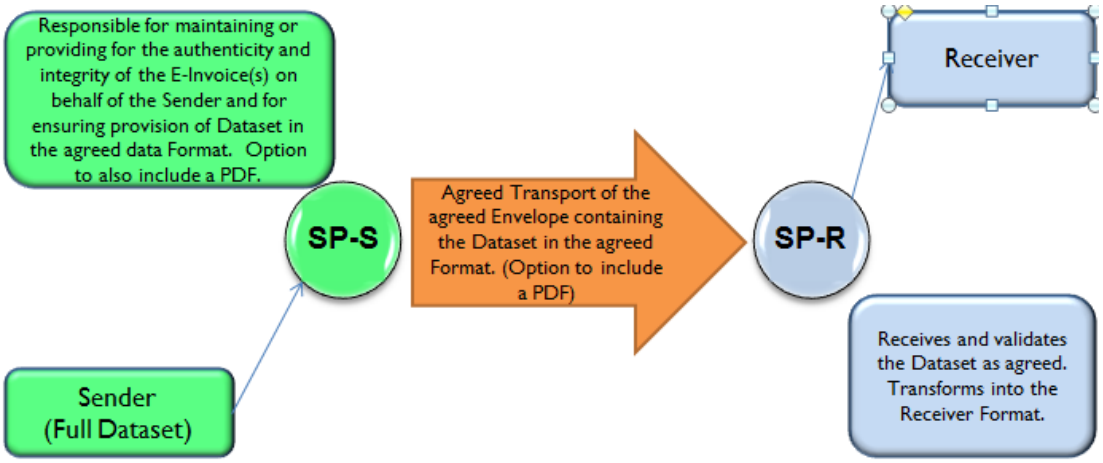
4. **Integrity of Content:** is demonstrated by:
   - Transmission within a secure network (Value added Network, AS2, x.400, Internet with authenticated accounts)
   - The Partner list: Which has to be coherent between Sending Party / Sender and Receiving Party / Receiver. Once committed, entries in a trading partner list cannot be altered.
   - A Summary list: Maintained individually on both sides with the list of invoices sent on the Sending Party / Sender side and the list of invoices received on the Receiving Party / Receiver side. Once committed, entries in a summary list cannot be altered. While mandatory in France (and other countries) this requirement may not be expected in some EU member states, however EESPA recommends maintaining a summary list as best practice.
   - As a consequence: The Partner list, the Summary list and the E-invoice exchanged (”original invoice”) must be archived on both sides.
   - **The integrity of the content is demonstrated by** the coherence and immutability of the trading partner list, summary list and e-Invoice between the Sending and the Receiving sides.

   The Summary list must contain the following (immutable) data:
   - Invoice number
   - Invoice Date
   - Date/Time of message creation
   - Net amount of invoice
   - Gross amount of invoice
   - Currency
   - The transmission system identification of the sender and receiver
   - The software version used

5. **Legibility:** Is the responsibility of each Party independently, for their respective customers. At the authorities’ request, the company (on behalf of their customer) must be able to reproduce the required data files sent or received during the legal retaining period. Reproducing an invoice message means presenting it in a format usually accepted for business purposes (human readable).

- **Checks & Controls** Levels 1, 2 and 3 as described earlier within this section.

MODE 3: Business Controls



Part 4.1 E-Invoice Message Payload Mode and Format Standard
In this Mode, Business Controls: (a) Compliance is based on EU VAT directive implementation and instructions. (b) The Sender and Receiver (Supplier and Buyer), working with their Service Provider as agreed, are responsible to implement "Business Controls", including audit trails, to show authorities and auditors that their accounting, book-keeping etc. are based on actual business transactions of goods and services (order, delivery, invoicing and payments). (c) The use of business controls creating a reliable audit trail between the invoice and the supply can be used to ensure the authenticity of origin, integrity of content and legibility for all invoices. (d) The Sending Party and Receiving Party are responsibility for the exchange of the E-Invoice Dataset. (e) The format and syntax of the dataset can be transformed by either the Sending or Receiving Party during the process. (f) An optional PDF view of the E-Invoice can be attached to the Structured File dataset. **1. E-Invoice creation:** ○ Mandatory Fields presence control: *See Appendix 1* ○ **Optional**: Additional validation (e.g. presence of specified references, such as purchase order or delivery note number): *<INCLUDE LIST HERE> and indicate action that would be taken where validation fails.* ○ Structured File generation: format defined in Payload section 2.
2. Payload Component (E-invoice exchanged): ○ E-invoice Format: Dataset in format agreed and recorded here. See Appendix 2 for default and recommended options. ○ Message envelope: *to be defined See Appendix 3 for default option*
3. Authenticity of Origin: Authenticity is achieved by maintaining auditable validation of the originator within the Services operated by the Sending Party and Receiving Party to ensure only e-Invoices from the correct Sender are received and processed.

4.	**Integrity of Content:** is achieved by validation of the data received from the Sender by the Sending Party and also by similar validation undertaken by the Receiving Party on behalf of the Receiver.
5.	**Legibility:** Legibility is achieved through the provision of either a PDF copy of the invoice or using the Invoice Dataset or by user access to view the E-Invoice on-line during the exchange process and within the agreed storage period.
6.	**Checks & Controls** Levels 1, 2 and 3 as described earlier within this section.

Completing Part 4.2: Business or Technical Acknowledgement or response Datasets in Message Payload

This is a free-format section within which details can be included to indicate the use of Business or Technical Acknowledgements or other response Datasets.

The anticipated use of this section would be to provide details to support the exchange of the EESPA Response Message (See Appendix 4 to this Companion). This section would confirm the use of the Response Message together with any agreed usage of status qualifiers within the Response Message:

Examples of documents that would be included within this section include:

1. The EESPA Response Message (See Appendix 4)
2. Others, as agreed by the Parties and detailed here.

Part 4.2 Business or Technical Acknowledgement or response Datasets in Message Payload
Example: 1. The EESPA Response Message will be used to provide status updates from the Receiving Party to the Sending Party for all Messages where status updates are available. 2. The Receiving Party may include any of the status elements identified within the EESPA Response Message (See Appendix 4 of the EESPA Companion to the MIA) 3. The Sending Party (of the e-Invoices) will convey the status details received within the EESPA Response Message to the Sender.

Completing Part 4.3: Other Electronic Business Documents in Message Payload

This is a free-format section within which details can be included to set out the mode of exchange for the Interoperability Services relating to documents other than Invoices (which are covered specifically within Part 4.1).

The exchange MODE may actually be very similar to the details within the MODE adopted in Part 4.1. However, the level of controls may be less rigid for non-invoice documents.

Examples of documents that would be included within this section include:

1. Purchase Order Messages
2. Application Integration (e.g. APERAK) Messages
3. Remittance Advice (e.g. REMADV) Messages

Part 4.3 Other Electronic Business Documents in Message Payload
Example: 1. The Receiving Party (of the e-Invoices) will send APERAK messages to the Sending Party (of the e-Invoices). 2. The Sending Party (of the e-Invoices) will receive the APERAK messages from the Receiving Party (of the e-Invoices) and convey these to the Sender (of the e-Invoices)

Completing Part 5: Set-Up and Service Procedures

Part 5. Set-Up and Service Procedures

This free-format section should be used, as required, to define the timing and nature of specific activities to be undertaken by each Party in setting up and maintaining the Interoperability Service. All of the items set out Paragraph 7 of the MIA covering Service Level and Support and in particular Paragraph 7.3, 7.4, 7.6 and 7.7 should be specified in this Part 5. Any workflow diagram and related descriptions that are agreed between the Parties should be placed in the section.

Example Procedure Elements for consideration:

1. The project timetable and milestones for establishing the Interoperability Services are:
    a) to undertake pilot exchange using test documents for all document types, in either or both sending and receiving directions as covered under this Model Interoperability Agreement (MIA) and to exchange the first test file within XX days of signing this MIA.
    b) to establish live exchange for the first pair of Customers using this MIA within XX days of signing the MIA and to complete the set-up of any Customers where these are specifically identified under this MIA within XX days of signing the MIA.
    c) All subsequent Interoperability Services requested to be established between a pair of Sending and Receiving Customers under this MIA will be implemented within XX days of the initial request being exchanged between the Parties.
2. The testing and sign-off process will be in accordance with the defined Interoperability Services within the MIA and Description of Services (DoS).
3. Document any agreed security procedures and requirements, as set out Paragraph 12.2 of the MIA.
4. The initial Set Up process for the first exchange of a document type in either direction will use test data and be undertaken within a test environment that replicates the live environment sufficiently to provide a valid result. Thereafter, new exchanges are to be implemented directly to live exchange unless mutually agreed by both Technical Contacts.
5. Activity reports will be provided by both the Sending and Receiving Party to the other Party on a calendar month basis within XX days of the end of each month and will include the number of transactions sent to, or received by, each Customer.
6. Any discrepancies identified within the activity reports to be notified within 1 calendar month of receipt. Both parties will work together in good faith to resolve any discrepancies within 1 calendar month of notification.
7. Each Party will maintain their System so that the availability of the Interoperability Services shall be over 95% within any 3 month period.
8. Maintenance or Upgrade activities which impacts upon the operation of the Interoperability Services other than for critical application maintenance, which shall include maintenance of the Interoperability Services required to achieve the agreed availability level indicated in point 7, will be notified by the Party undertaking the Maintenance or Upgrade activities to the other Party with at least 48 hours' notice.
9. Communication between the Parties relating to these Set-up and Service Procedures will be exchanged between the Technical Contacts identified in Part 1 using Email exchange where this is to notify of either completion, change or delay of any activities identified within this section of the DoS.

Completing Part 6: Charges

This is a free-format section to allow the Parties to set out any mutually agreed charges that will apply between the Parties relating to the provision of the Interoperability Service, as is provided for in Paragraph 10 of the MIA. These ONLY relate to charges between the Parties and NOT to charges each may apply to their own Customers, even where these are as a direct consequence of charges included within this Part 6.

The table below is only intended to give an example of details that could be included here.

Part 6. Charges
Examples: **1.** A charge of €xxx will be payable by the Sending Party to the Receiving Party for each Invoice or Electronic Business Document exchanged and acknowledged as received. **2.** All payments due under this Part 6 will be payable quarterly in arrears based on invoices received.

Completing Part 7: Certification of Internal Controls

This is a free-format section which, if required, can be used to define any certification that either or both Parties maintains and is prepared to share with the other Party, together with the ways in which each Party agrees to provide to the other Party evidence of any Certification of its internal controls (Certification), as set out in Paragraph 12.6 of the MIA.

An example would be the ISAE3402 (replacement for SAS70).

Part 7. Certification of Internal Controls
Examples: **1a. Neither** party supports third party certification. **1b. Party** A supports Certification HHHH and will make available a copy of the certificate from the awarding body on an annual basis. **1c.** Both Parties support the following Certification and will allow an annual site inspection of the Certification subject to 4 weeks' notice. a. HHHH b. JJJJJ

Completing Part 8: Other Specified Terms and Conditions

This is a free-format section which, if required, can be used to define any additional terms or conditions that both Parties agree to include within this Model Interoperability Agreement.

Part 8. Other Specified Terms and Conditions
Examples: **1.** Any additional Indemnities and Warranties, such as relating to items within Section 8.4 of the MIA. **2.** Any Service Level Agreement **3.** Agreement to use a Governing Law other than Belgium (Default in the Agreement), as provided for in Paragraph 21.1 of the MIA. **4.** Specific Agreement on Data Protection procedures as set out in the MIA as set out in Paragraph 14.1 of the MIA.

Section E Appendixes

Appendix 1 - Mandatory Fields (EU Directive)

VAT Directive Mandatory fields

(1) the date of issue;

(2) a sequential number, based on one or more series, which uniquely identifies the invoice;

(3) the VAT identification number referred to in Article 214 under which the taxable person supplied the goods or services;

(4) the customer's VAT identification number, as referred to in Article 214, under which the customer received a supply of goods or services in respect of which he is liable for payment of VAT, or received a supply of goods as referred to in Article 138;

(5) the full name and address of the taxable person and of the customer;

(6) the quantity and nature of the goods supplied or the extent and nature of the services rendered;

(7) the date on which the supply of goods or services was made or completed or the date on which the payment on account referred to in points (4) and (5) of Article 220 was made, in so far as that date can be determined and differs from the date of issue of the invoice;

(8) the taxable amount per rate or exemption, the unit price exclusive of VAT and any discounts or rebates if they are not included in the unit price;

(9) the VAT rate applied;

(10) the VAT amount payable, except where a special arrangement is applied under which, in accordance with this Directive, such a detail is excluded;

(11) in the case of an exemption or where the customer is liable for payment of VAT, reference to the applicable provision of this Directive, or to the corresponding national provision, or any other reference indicating that the supply of goods or services is exempt or subject to the reverse charge procedure;

VAT Directive “Dependent” Fields (Mandatory if conditions for use exist)

The use of these fields depends on the specific situation relating to the supplier or the content of the invoice. As a result, these fields are not easy to check for a Service Provider.

(12) in the case of the supply of a new means of transport made in accordance with the conditions specified in Article 138 (1) and (2)(a), the characteristics as identified in point (b) of Article 2(2);

(13) where the margin scheme for travel agents is applied, reference to Article 306, or to the corresponding national provisions, or any other reference indicating that the margin scheme has been applied;

(14) where one of the special arrangements applicable to second-hand goods, works of art, collectors' items and antiques is applied, reference to Articles 313, 326 or 333, or to the corresponding national provisions, or any other reference indicating that one of those arrangements has been applied;

(15) where the person liable for payment of VAT is a tax representative for the purposes of Article 204, the VAT identification number, referred to in Article 214, of that tax representative, together with his full name and address.

Other Mandatory fields

Local requirements or additional fields related to Trade Law (which are, in general, mandatory fields within the payload, such as:

- Type of legal structure for the Sender + Capital
- Payment Date / mean of payment
- Total Amount

Appendix 2 - Data formats

EESPA default data format

Format: **UBL 2.0 syntax based on the semantic model of CEN BII2**

Profile ID: **BII04 – Invoice Only**

Transaction: **BiiTrns010**

Introduction

EESPA promotes the use of the CEN BII2, UBL2.0 syntax as defined by the CEN Workshop Agreement 16073-0.

- All information on CEN BII2 can be found here: http://www.cenbii.eu/
- The Information Requirement Model which defines the detailed information requirements in order to fulfill the business requirements can be found here: http://www.cenbii.eu/wp-content/uploads/BiiTrns10-IRM.rtf.
- The profile specification which describes the overall business process as well as the business requirements related to that process can be found here: http://www.cenbii.eu/wp-content/uploads/Profile-BII2-04-Invoice-only.pdf
- The mapping of the CEN BII2 with the UBL 2.0 syntax can be found here: http://www.cenbii.eu/wp-content/uploads/BiiTrns10-SB-UBL.rtf.
- The code lists are available at: http://www.cenbii.eu/wp-content/uploads/BII2-Code-Lists.xls
- XSD Scheme of UBL2.0 can be found here: http://docs.oasis-open.org/ubl/os-UBL-2.0/xsd/maindoc/UBL-Invoice-2.0.xsd
- Tools to check the UBL 2.0 invoice against the CEN BII rules: http://www.cen.eu/cwa/bii/specs/Tools/index.html
- Link to implementation aids for UBL: http://www.simpleubl.com/
- And an example of a UBL 2.0 / BiiCoreTrdm010 can be found here: http://connect.demo.ibxplatform.com/Connect/xml/EHF%20Invoice%20example%20simple.xml

Mapping of the mandatory invoice fields

The following is an EESPA default mapping to relevant invoice fields, mandatory from a legal point of view or recommended from a business point of view. The list is not final yet and will be updated by EESPA based on shared experience.

Data contents	Core / Country / Industry	Mandatory / Dependent / Recommended / Optional	Article/ paragraph VAT directive 2006/112/ EC	CENBII CORE Invoice	Comment
Header section					
Invoice type	Core	Mandatory (UBL)		Invoice/cbc:InvoiceTypeCode	Commercial Invoice: 380 Factored invoice: 393 .Note that for Credit notes, the following profile should be used: BiiTrns014 Credit Note
Document currency	Core	Mandatory		Invoice/cbc:DocumentCurrencyCode	Preferably ISO-code
Date of issue	Core	Mandatory	226/1	Invoice/cbc:IssueDate	Invoice date
Sequential number based on one or more series which uniquely identifies the invoice	Core	Mandatory	226/2	Invoice/cbc:ID	Invoice Number
VAT identification number for supplier	Country	Dependent	226/3	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PartyTaxScheme/cbc:CompanyID	If supplier is VAT registered
VAT identification number for customer received the goods	Country	Dependent	226/4	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PartyTaxScheme/cbc:CompanyID	Depending on country legal requirements this field is mandatory
Full name of supplier (Company)	Core	Mandatory	226/5	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PartyName/cbc:Name	Supplier Company Name
Street address of supplier	Core	Mandatory	226/5	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PostalAddress/cbc:StreetName	Address line 1
Street address of supplier	Industry	Optional		Invoice/cac:AccountingSupplierParty/cac:Party/cac:PostalAddress/cbc:AdditionalStreetName	Address line 2
Postal code of supplier	Core	Mandatory	226/5	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PostalAddress/cbc:PostalZone	
Town of supplier	Core	Mandatory	226/5	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PostalAddress/cbc:CityName	

Country of supplier	Core	Mandatory	226/5	Invoice/cac:AccountingSupplierParty/cac:Party/cac:PostalAddress/cac:Country/cbc:IdentificationCode	Preferably ISO code
Full name of Customer (Company)	Core	Mandatory	226/5	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PartyName/cbc:Name	Customer Company name
Street address of receiving customer	Core	Mandatory	226/5	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PostalAddress/cbc:StreetName	Address line 1
Street address of receiving customer	Industry	Optional		Invoice/cac:AccountingCustomerParty/cac:Party/cac:PostalAddress/cbc:AdditionalStreetName	Address line 2
Postal code of receiving customer	Core	Mandatory	226/5	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PostalAddress/cbc:PostalZone	
Town of receiving customer	Core	Mandatory	226/5	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PostalAddress/cbc:CityName	
Country of receiving customer	Core	Mandatory	226/5	Invoice/cac:AccountingCustomerParty/cac:Party/cac:PostalAddress/cac:Country/cbc:IdentificationCode	Preferably ISO code
Deliver to location identifier	Industry	Optional		Invoice/cac:Delivery/cac:DeliveryLocation/cbc:ID	Can be used to identify a specific Depot number or dock
Deliver to streetname	Core	Dependent		Invoice/cac:Delivery/cac:DeliveryLocation/cac:Address/cbc:StreetName	If delivery address is not equal to customer address
Deliver to streetname2	Industry	Optional		Invoice/cac:Delivery/cac:DeliveryLocation/cac:Address/cbc:AdditionalStreetName	
Postal code of delivery address	Core	Dependent		Invoice/cac:Delivery/cac:DeliveryLocation/cac:Address/cbc:PostalZone	
Town of delivery address	Core	Dependent		Invoice/cac:Delivery/cac:DeliveryLocation/cac:Address/cbc:CityName	
Country of delivery address	Core	Dependent		Invoice/cac:Delivery/cac:DeliveryLocation/cac:Address/cac:Country/cbc:IdentificationCode	
Purchase Order Reference	Industry	Recommended		Invoice/cac:OrderReference/cbc:ID	Order reference identifier, should always be on header level
Contract Reference	Industry	Optional		Invoice/cac:AccountingCustomerParty/cac:Party/cac:Contact/cbc:ID	Field can be used if additional references are given by the buyer, such as reference to a supply contract
Date of supply of goods or services	Core	Mandatory	226/7	Invoice/cbc:TaxPointDate	Date on which the goods were delivered

Amount of prepayment	Core	Dependent		Invoice/cac:LegalMonetaryTotal/cbc:PayableAmount	Fill this if prepayments were received
Line item section					
PO Line item number	Industry	Recommended		Invoice/cac:InvoiceLine/cac:OrderLineReference/cbc:LineID	Reference to the purchase order line number
Product code supplier	Industry	Recommended		Invoice/cac:InvoiceLine/cac:Item/cac:SellersItemIdentification/cbc:ID	Item identifier as defined by the seller
Standard product code	Industry	Optional		Invoice/cac:InvoiceLine/cac:Item/cac:StandardItemIdentification/cbc:ID	Universal product code
Quantity of goods or extent of services	Core	Mandatory	226/6	Invoice/cac:InvoiceLine/cbc:InvoicedQuantity	
Unit of quantity or extent	Core	Mandatory	226/6	UnitCode attribute for previous	Unit of Measure for invoice item
Nature (description) of goods or services	Core	Mandatory	226/6	Invoice/cac:InvoiceLine/cac:Item/cbc:Name	Line Item description
Unit price exclusive of VAT	Core	Mandatory	226/8	Invoice/cac:InvoiceLine/cac:Price/cbc:PriceAmount	Unit Price per Unit of Quantity or Extent (Measure)
Discounts or rebates if not included in unit price	Core	Dependent	226/8	Invoice/cac:InvoiceLine/cac:AllowanceCharge/cbc:Amount	In case discount or rebates are given
Applied VAT rate	Core	Mandatory	226/9	Invoice/cac:InvoiceLine/cac:Item/cac:ClassifiedTaxCategory/cbc:Percent	
Applied VAT code	Industry	Recommended		Invoice/cac:InvoiceLine/cac:Item/cac:ClassifiedTaxCategory/cbc:ID	See code UBL code list
Invoice line net amount	Industry	Recommended		Invoice/cac:InvoiceLine/cbc:LineExtensionAmount	Total amount of line item including discounts and rebates but excluding VAT
VAT amount payable	Core	Mandatory	226/10	Invoice/cac:InvoiceLine/cac:TaxTotal/cbc:TaxAmount	Total amount of VAT
Taxable amount per rate	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cbc:TaxableAmount	Summary of taxable amount per rate
Tax amount	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cbc:TaxAmount	
Vat category code	Industry	EESPA Best Practice	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:ID	Preferably use UBL code list
VAT category percentage	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:Percent	
Reason for exemption	Core	Dependent	226/11	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:TaxExemptionReason	See applied VAT code – preferably use exemption code
Allowance and charge reason	Core	Recommended		Invoice/cac:AllowanceCharge/cbc:AllowanceChargeReason	

Allowance and charge Tax category	Industry	Recommended		Invoice/cac:AllowanceCharge/cac:TaxCategory/cbc:ID	See UBL code list
Allowance and charge Tax percentage	Core	Recommended		Invoice/cac:AllowanceCharge/cac:TaxCategory/cbc:Percent	
Line extension amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:LineExtensionAmount	Total of all net line item amounts
Total allowance amount	Core	Dependent		Invoice/cac:LegalMonetaryTotal/cbc:AllowanceTotalAmount	
Total charge amount	Core	Dependent		Invoice/cac:LegalMonetaryTotal/cbc:ChargeTotalAmount	
Total net amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:TaxExclusiveAmount	Total of invoice including all charges and allowances and excluding VAT
Total VAT amount	Core	Mandatory		Invoice/cac:TaxTotal/cbc:TaxAmount	Total VAT amount
VAT in local currency	Core	Dependent		Invoice/cac:TaxTotal/cbc:TaxAmount	Tax total in local currency, only required in case of invoices in foreign currency
Total invoice amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:TaxInclusiveAmount	Total of invoice
Totals section					
Taxable amount per rate	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cbc:TaxableAmount	Summary of taxable amount per rate
Tax amount	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cbc:TaxAmount	
Vat category code	Industry	EESPA Best Practice	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:ID	Preferably use UBL code list
VAT category percentage	Core	Mandatory	226/8	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:Percent	
Reason for exemption	Core	Dependent	226/11	Invoice/cac:TaxTotal/cac:TaxSubtotal/cac:TaxCategory/cbc:TaxExemptionReason	See applied VAT code – preferably use exemption code
Allowance and charge reason	Core	Recommended		Invoice/cac:AllowanceCharge/cbc:AllowanceChargeReason	
Allowance and charge Tax Amount		Dependent		Invoice/cac:AllowanceCharge/cac:TaxCategory/cbc:ID	See UBL code list
Allowance and charge Tax category	Industry	Recommended		Invoice/cac:AllowanceCharge/cac:TaxCategory/cbc:ID	See UBL code list

Allowance and charge Tax percentage	Core	Recommended		Invoice/cac:AllowanceCharge/cac:TaxCategory/cbc:Percent	
Line extension amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:LineExtensionAmount	Total of all net line item amounts
Total allowance amount	Core	Dependent		Invoice/cac:LegalMonetaryTotal/cbc:AllowanceTotalAmount	
Total charge amount	Core	Dependent		Invoice/cac:LegalMonetaryTotal/cbc:ChargeTotalAmount	
Total net amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:TaxExclusiveAmount	Total of invoice including all charges and allowances and excluding VAT
Total VAT amount	Core	Mandatory		Invoice/cac:TaxTotal/cbc:TaxAmount	Total VAT amount
VAT in local currency	Core	Dependent		Invoice/cac:TaxTotal/cbc:TaxAmount	Tax total in local currency, only required in case of invoices in foreign currency
Total invoice amount	Core	Mandatory		Invoice/cac:LegalMonetaryTotal/cbc:TaxInclusiveAmount	Total of invoice

Explanation of the columns

- Data contents: Comprehensible description of the business requirement
- Core/Country/Industry: Indication on the level on which the business requirement is defined:
  - Core: EU-level
  - Country: country level
  - Industry: specific for a specific industry (group)
- Mandatory/Dependent/Recommended/Optional: is the business requirement:
  - Mandatory: should always be filled
  - Dependent: to be used if the conditions apply
  - Recommended: according to EESPA best practices the use is recommended
  - Optional: if the business requirement exists, EESPA recommends the use of the related field
- Article/ paragraph VAT directive 2006/112/EC: reference to the Directive text for the legally mandatory fields
- CENBII CORE Invoice: mapping of the business requirement to the UBL2.0 field.
- Comment: extra information where needed.

Remarks:

- For credit notes the profile BiiTrns014 Credit Note from CENBII should be used. In the current version of the companion document, no guidelines are given by the EESPA as to how the profile should be implemented. The usage and the way it is used is subject to bilateral agreement between service providers.
- Shipped from address is not foreseen in the standard. If required then service providers will need to agree on a bilateral basis on the field to be used.

Mapping from UBL to other data formats

Cross-references of the data-elements to the Cross Industry Invoice (UN/CEFACT XML) can be found on http://www.cenbii.eu/wp-content/uploads/BiiTrns10-SB-Cefact.rtf

Description of alternative data standards

VeR EDIFACT

Version: **Based on EDIFACT D01 B.**

Subset: **VeR (E-Invoicing Alliance, Germany)**

This standard has been evaluated by the EESPA technical working group to verify that this would:

- Defined and open standard available to be adopted
- Fulfil tax & legal requirements
- International approach
- Governance model / maintenance procedure
- Integration with upstream process (supply chain)
- Integration with downstream process (payment)
- SME focus vs. elite solution (all discussed formats somehow the same)

This standard was chosen and defined by VeR as a common standard for e-Invoicing. The criteria for adopting this standard were:

- A cross-industry standard
- Detailed documentation and business rules available
- A mature format with significant adoption
- Ability to influence the development of the standard
- Ability to support different uses, such as:
    - Core: minimum requirements for a legal invoice (without order reference)
    - Enhanced: including booking information for automated processing (with order reference)
    - Bilateral: Using segments that are project depending and require an agreement between Provider A and B

Implementation Documentation:

a. 20091218_VeR Implementation Guide INVOIC V 1.0.xls

b. 20091218_VeR Musterrechnung 471102.xlsx

c. VER_Inhaltsstandard_V1.1_eng.PDF

ISO 20022

Version: **ISO 20022 Financial Invoice Message**

Subset: **FinancialInvoiceV01 submitted by UN/CEFACT TBG5**

This standard has been evaluated by EESPA technical working group to verify that it is:

- Defined and open standard available to be adopted
- Fulfils tax & legal requirements
- Global approach
- Governance model/maintenance procedure provided by the ISO 20022 organization
- Integration with upstream process (orders)
- Integration with downstream process (compatible with Single Euro Payment Area SEPA payment traffic)
- Based on enterprise needs while providing good SME support

Global ISO 20022 Financial Invoice Message is developed according to the ISO 20022 standard. There is detailed documentation and business rules available for implementing the format at www.ISO20022.org. It has high performance and it is in use in practice.

ISO20022 Financial Invoice Message is XML based subset of Cross Industry Invoice (CII). It mostly uses the same names and element definitions as CII to make mapping easier. It is structured to reflect the hierarchy of the Core Invoice and CII from Header to Line Items.

The following are typical business scenarios that ISO20022 e-invoice addresses (other scenarios are also possible to support): Request for payment, Invoice Factoring scenario, Electronic Bill Payment & Presentment (EBPP) scenario, e-Invoicing via Service Provider scenario and Supply Chain Financing scenario.

ISO 20022 Financial Invoice Message does not include required structure and content for addressing and message routing. It is recommended to use GS1 SBDH header structure as a generic structure for addressing. There is documentation and samples available on how to combine ISO 20022 Financial invoice with SBDH Header.

Implementation Documentation:

a. XML Schema

b. Business examples of XML instances

c. Message Definition Report

d. Diagrams (business flows, messages, scenarios)

e. GS1 SBDH header structure (http://www.gs1tw.org/twct/gs1w/download/SBDH_v1.3_Technical_Implementation_Guide.PDF)

Note: *Tieto has adopted a version produced under the Single Face To Industry (SFTI) initiative, which is a joint undertaking in the Swedish public sector to promote and facilitate e-procurement. The main SFTI change compared to the GS1 version is that payload cardinality has been changed to unbounded to allow for multiple payloads. An English version translated by Tieto (SFTI Guide for SBDH) has been provided by Tieto and is available from EESPA.*

To access documents (a-d):

1) Go to http://www.iso20022.org/trade_services_messages.page
2) See Financial Invoice under the section:
   "List of ISO 20022 Trade Services message definitions per message set" (mid-page)
3) Click on the "+" sign for "Trade Services Initiation"
4) Here you will find the ISO documents and zip files for this standard

Appendix 3 - Envelope Standard

Format: **The GS1 "Standard Business Document Header" (SBDH)**

Version: **1.3**

General description

- The SBDH is independent from the content format and permits the transport of structured data and PDF files.
- The SBDH supports multi party addressing without looking into the structured data, is well defined and in practical use.
- The use of a **filename for the SBDH** is optional. Where used, this must be in the following format, unless agreed by both Parties and included within Section 3 of the Description of Services. The ID's referenced within the SBDH filename must be the same as those used within this SBDH itself.
  SBDH Filename Format:
  - Sending Party Addressing ID_Sender's ID_Receiving_Party Addressing ID_Receiver's ID_Creation Date/Time
  - EESPA Sending and Receiving Party ID's are defined within Appendix 5 of this Companion.
  - ... with the Date/Time in the CCYYMMDDHHMMSSTTT format.
    - C=Century, Y=Year, MM=Month, DD=Day, HH=Hour, MM=Minute: SS=Seconds, TTT=Thousandths of a Second
  - E.g. 2234_5015266354552_8712_1234567890128_201304221305000

The EESPA deployment of the SBDH focuses on routing and transport needs.

Encryption and signature options of the SBDH definition should not be used for the following reasons:

- The SBDH allows selective encryption, which is available using the XML Encryption specification in different variations. EESPA suggests not using this encryption. The security of the data should be covered by the transport protocol (AS2, VAN etc.).
- Also, it would be possible, to sign the whole SBDH envelope. If this signature would be used for legal aspects, the whole envelope would need to be archived. If signatures are used, they should be included in the payload (PDF signature, signature included in structured payload) or sent as a separate attachment in the envelope in PK7 format.
- The envelope is able to transport many signatures (payload and additional attachment can be signed). Only one signature should be added (if defined by the mode) at the payload level.

References

GS1 XML Message Architecture Implementation Guide Issue 1, July-2009
http://www.gs1au.org/assets/documents/products/gs1_system/gs1_emess_xml_implementation.PDF

Standard Business Document Header (SBDH) Version 1.3 Technical Implementation Guide *Issue 1, July-2007*
http://www.gs1tw.org/twct/gs1w/download/SBDH_v1.3_Technical_Implementation_Guide.PDF

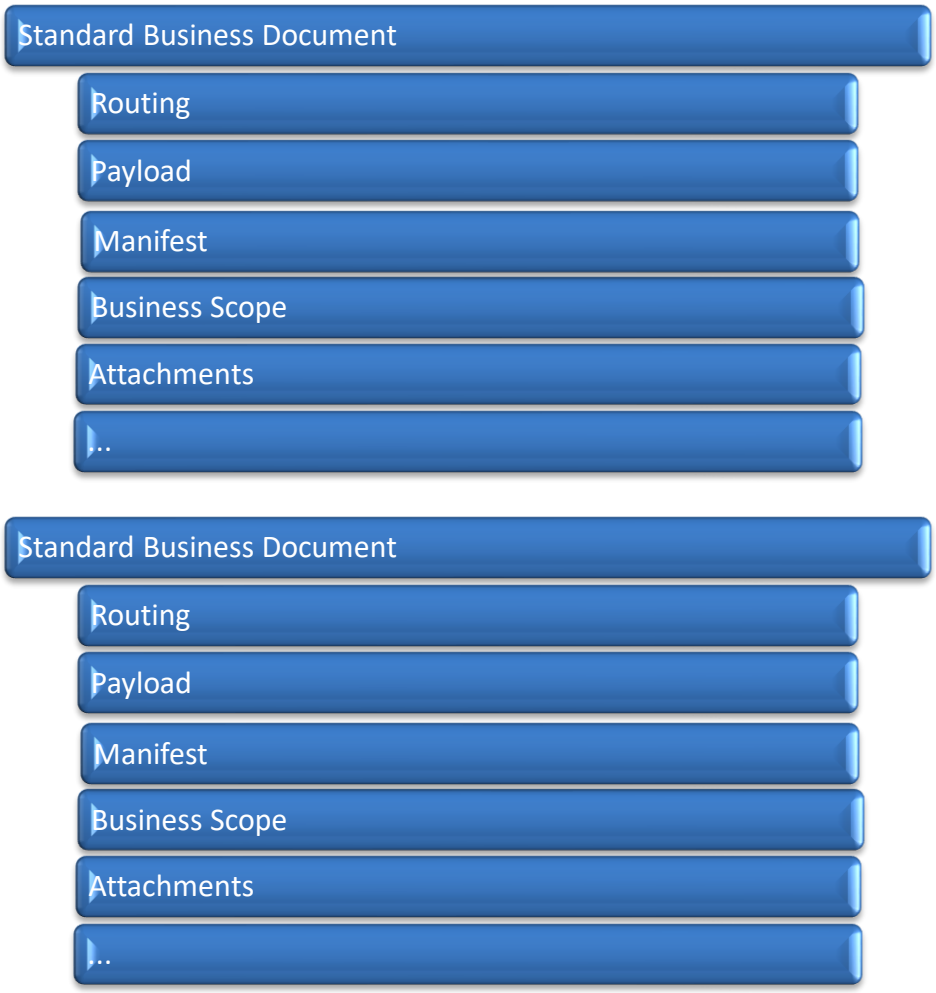


Figure 1. Structure of the Standard Business Document Header (SBDH)

Routing

Document routing information is captured in the 'Sender' and 'Receiver' data structures. This identifies the Sender and Receiver using unique "Addressing ID's" for both the Customers and the "Routing ID's" for each Service Provider.

Details for the EESPA "Addressing & Routing" protocol are included within Appendix 5 of this Companion.

Identification Tags used by EESPA within the SBDH:

Sender/Identifier: The Addressing ID of the sender as defined within Section 3 of the Description of Services.

Receiver/Identifier: The Addressing ID of the receiver as defined within Section 3 of the Description of Services.

Authority Qualifiers used by EESPA with Identification Tags within the SBDH

NOTE: The inclusion of an "Authority" qualifier is optional. The use made of Authority qualifiers must be defined by the Parties within Section 3 of the Description of Services.

The EESPA recommended qualifiers listed below would be inserted at the position shown as "XXX" in the example included below:

QUALIFIER	DESCRIPTION
"EAN.UCC"	= The ID is a GLN
"VATIN"	= The ID is a VAT Number
"EESPA"	= The ID is an EESPA defined reference for the Customer
"COUNTRYCODE:ORGANISATIONIDENTIFIER"	= Country Code (ISO 2 Digit) & Organisation ID (e.g. DE54223332)
"NONE"	= No qualifier provided for this ID

Others could be agreed by the Parties and defined within the Description of Services.

Example:

```
<cefact:Sender>
    <cefact:Identifier Authority="XXX">6902345899128</cefact:Identifier>
</cefact:Sender>
<cefact:Receiver>
    <cefact:Identifier Authority="XXX">5099344477362</cefact:Identifier>
</cefact:Receiver>
```

Payload

Payload is the container area provided to include the business documents. The payload area can be used to hold any kind of content. The "original" invoice is defined as payload. This will depend on the Mode adopted but the default EESPA option, for example, defines the Original Invoice as the PDF. In which case, the payload is a PDF. Where only a Dataset is exchanged, this would then be the Payload.

The "DocumentIdentification" node is used to define the payload.

In the EESPA case, the payload is compound from the *attachment* nodes (as many as there are) and, optionally, the *signature* node.

Tags used by EESPA:

Standard:	PDF, EDIFACT, CEN UBL BII, ISO20022, EESPA (e.g. for the XML Response Messages)
TypeVersion:	Version of the file format (optional)
InstanceIdentifier:	Unique message number (optional)
Type:	Fix INVOIC (for invoices and credit notes). Other document types can be defined bilateral. [Response]

CreationDateAndTime: The date and time the envelope is created

Example:

```
<cefact:DocumentIdentification>
  <cefact:Standard>EDIFACT</cefact:Standard>
  <cefact:TypeVersion>D.07A</cefact:TypeVersion>
```

```
<cefact:InstanceIdentifier>2011-09-05T11:47_001</cefact:InstanceIdentifier>
<cefact:Type>INVOIC</cefact:Type>
<cefact:CreationDateAndTime>2011-09-01T12:10:10</cefact:CreationDateAndTime>
</cefact:DocumentIdentification>
```

Manifest

This section is used to define the number of attachments and their filenames

Tags used by EESPA:

NumberOfItems:	the number of attachments (including the payload)
MimeTypeQualifierCode:	the mime type of the attachment. The possible mime types in EESPA are defined in the following section.
UniformResourceIdentifier:	[“number of the document”” –””document name incl. suffix”]

Example:

This example contains 2 attachments in different MimeTypes.

```
<cefact:Manifest>
<cefact:NumberOfItems>2</cefact:NumberOfItems>
<cefact:ManifestItem>
<cefact:MimeTypeQualifierCode>application/EDIFACT</cefact:MimeTypeQualifierCode>
<cefact:UniformResourceIdentifier>1 - INVOICE_12345.EDI</cefact:UniformResourceIdentifier>
</cefact:ManifestItem>
<cefact:ManifestItem>
<cefact:MimeTypeQualifierCode>application/PDF</cefact:MimeTypeQualifierCode>
<cefact:UniformResourceIdentifier>2 – INVOICE_12345.PDF</cefact:UniformResourceIdentifier>
</cefact:ManifestItem>
</cefact:Manifest>
```

Business Scope

This section is used to specify the EESPA Mode that has been used for interoperability relating to this Envelope. The definition of the Mode clarifies if the payload is signed or not and how the processing of the files included in the envelope should be done.

Tags used by EESPA:

Type: fix “BusinessProcess”
Identifier: fix “EESPA Interoperability Mode”
InstanceIdentifier: The EESPA mode defined in this document

Example:

```
<cefact:BusinessScope>
        <cefact:Scope>
                <cefact:Type>BusinessProcess</cefact:Type>
                <cefact:Identifier>EESPA Interoperability Mode</cefact:Identifier>
                <cefact:InstanceIdentifier>1a</cefact:InstanceIdentifier>
         </cefact:Scope>
</cefact:BusinessScope>
```

This example identifies that the SBDH is following the 1a Mode specifications (signed PDF + dataset) and therefore how it would be validated/archived/processed. This ability to distinguish between Modes is particularly useful when differentiating between modes 2 and 3 (both unsigned structured data). The sub cases of a mode can be identified using the mime types of the payload and the attachments.

Attachments

All documents included in the envelope are sent as attachments.

An attachment can be:

- The payload (Mandatory)
- Additional attachments (PDF, XML Response Message)
- A separate signature file (PK7 file)

Each attachment has an encoding specified in the node Attachment Encoding (in EESPA always Base64). The first attachment is defined to be the payload.

Tags used by EESPA:

Attachment Encoding: *fix “http://www.w3.org/2000/09/xmldsig#base64”*

Id: *the number of the document in the envelope “ID_1”= the first attachment in the envelope*

MimeType: *the mime type of the attachment. The possible mime types in EESPA are defined in the* following section. The document itself is added after this definition.

Example:

This example contains 2 attachments in different MimeTypes.

```
<Attachment Encoding="http://www.w3.org/2000/09/xmldsig#base64" Id="ID_1" MimeType="application/octet-stream">VU5BOisuPyAnVU5Q2NT…….. </Attachment>
 <Attachment Encoding="http://www.w3.org/2000/09/xmldsig#base64" Id="ID_2" MimeType="application/PDF">JVBERi0xLjUNCiW1tbW1DQoxIDAgb2Jq…….. </Attachment>
```

Use of the Envelope with Mode 1a

In Mode 1a, the Sending Party receives a full invoice dataset from the Sender. The original document is the PDF file. The Sending Party creates the E-Invoice (PDF + dataset) on behalf of the Sender.

1. PDF (Signed):

    - PDF file - MimeTypeQualifierCode: application/PDF

2. Attached pkcs7 signature (containing PDF)

    - pkcs7 file - MimeTypeQualifierCode: application/pkcs7-mime

3. Detached pkcs7 signature

    - PDF file - MimeTypeQualifierCode: application/PDF

    - signature file - MimeTypeQualifierCode: application/pkcs7-signature

Sub Mode	Document Identification/ Standard	ManifestItem/ MimeTypeQualifierCode	Additional Attachment	Signature Attachment
1	PDF	application/PDF	structured file*	none
2	PDF	application/PDF	structured file*	application/pkcs 7-mime (suffix ".pk7")
3	PDF	application/PDF	structured file*	application/pkcs 7-signature (suffix ".p7S")

*As structured data, the EESPA default is CEN BII.

Format	ManifestItem/MimeTypeQualifierCode
CEN BII	application/xml

Sample xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<StandardBusinessDocument
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:cefact="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader"
xmlns:ds="http://www.w3.org/2000/09/xmldsig"
xmlns:mime="http://www.w3.org/2005/05/xmlmime"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.eespa.eu/namespaces/StandardBusinessDocumentHeader StandardBusinessDocumentHeader1p3.xsd">
 <cefact:HeaderVersion>1.3</cefact:HeaderVersion>
 <cefact:Sender>
```

```
 <cefact:Identifier Authority="EAN.UCC"> 5015266354552</cefact:Identifier>
 </cefact:Sender>
 <cefact:Receiver>
  <cefact:Identifier Authority="NONE">1234567890128</cefact:Identifier>
 </cefact:Receiver>
 <cefact:DocumentIdentification>
  <cefact:Standard>EDIFACT</cefact:Standard>
  <cefact:TypeVersion>D.07A</cefact:TypeVersion>
  <cefact:InstanceIdentifier>2011-09-05T11:47_001</cefact:InstanceIdentifier>
  <cefact:Type>INVOIC</cefact:Type>
  <cefact:CreationDateAndTime>2011-09-01T12:10:10</cefact:CreationDateAndTime>
 </cefact:DocumentIdentification>
 <cefact:Manifest>
  <cefact:NumberOfItems>2</cefact:NumberOfItems>
  <cefact:ManifestItem>
   <cefact:MimeTypeQualifierCode>application/EDIFACT</cefact:MimeTypeQualifierCode>
   <cefact:UniformResourceIdentifier>1 - INVOICE_12345.EDI</cefact:UniformResourceIdentifier>
  </cefact:ManifestItem>
  <cefact:ManifestItem>
   <cefact:MimeTypeQualifierCode>application/PDF</cefact:MimeTypeQualifierCode>
   <cefact:UniformResourceIdentifier>2 - INVOICE_12345.PDF</cefact:UniformResourceIdentifier>
  </cefact:ManifestItem>
 </cefact:Manifest>
<cefact:BusinessScope>
 <cefact:Scope>
    <cefact:Type>BusinessProcess</cefact:Type>
    <cefact:Identifier>EESPA Interoperability Mode</cefact:Identifier>
    <cefact:InstanceIdentifier>3</cefact:Identifier>
 </cefact:Scope>
</cefact:BusinessScope>
 </cefact:StandardBusinessDocumentHeader>
<AttachmentEncoding="http://www.w3.org/2000/09/xmldsig#base64"Id="ID_1"MimeType="application/EDIFACT">VU5BOisuPyAnVU5Q2NT
.....</Attachment>
 <Attachment Encoding="http://www.w3.org/2000/09/xmldsig#base64" Id="ID_2" MimeType="application/PDF">
JVBERi0xLjUNCiW1tbW1DQoxIDAgb2Jq.....</Attachment>
</StandardBusinessDocument>
```

The usage of the SBDH with other EESPA modes

For the different interoperability Modes, the envelope contains different files in several formats. The Mode used is defined in “BusinessScope” section of this Appendix.

The following section explains the tags used by some of the EESPA Modes:

Mode 1b: Digital signature applied on dataset (with or without a PDF file attached)

In this mode, the Sending Party receives from the Sender a full invoice dataset. The Sending Party creates the E-Invoice on behalf of the Sender. A PDF can be attached to the Structured File dataset. The PDF can be generated by the Sending Party or directly by the Sender (in general this is formatted to the same template as the paper invoice). The dataset is signed. The PDF may optionally be signed. In some markets, formats are used that contains the signature in the structured file itself. The verification of these signatures has to be implemented for each format and is therefore not recommended by EESPA

1. Signature included in structured file (e.g. factura E or Edifact signatures, not recommended)
   - Optional PDF file - MimeTypeQualifierCode: application/PDF
2. Attached pkcs7 signature (containing structured file)
   - Optional PDF file - MimeTypeQualifierCode: application/PDF
   - pkcs7 file - MimeTypeQualifierCode: application/pkcs7-mime
3. Detached pkcs7 signature
   - Optional PDF file - MimeTypeQualifierCode: application/PDF
   - Signature file - MimeTypeQualifierCode: application/pkcs7-signature

Sub Mode	Document Identification/ Standard	ManifestItem/ MimeTypeQualifierCode	Additional Attachment	Signature Attachment
1	XML or EDIFACT	application/xml application/EDIFACT	PDF (opt.)*	none
2	XML or EDIFACT	application/xml application/EDIFACT	PDF (opt.)*	application/pkcs 7-mime (suffix ".pk7")
3	XML or EDIFACT	application/xml application/EDIFACT	PDF (opt.)*	application/pkcs 7-signature (suffix ".p7S")

*PDF mime type (optional)

Format	ManifestItem/MimeTypeQualifierCode
PDF	application/PDF

Mode 2: Based on EDI

In this mode, the Sending Party receives from the Sender a full invoice dataset. The Sending Party creates the E-Invoice on behalf of the Sender in a structured File Format without a digital signature. Authenticity of the origin and integrity of the content are guaranteed by a mutual fulfilment of a Partner list (a list of e-Invoicing trading partners

for this mode) and Summary list with dates and identification of the sender and receiver that preserves the identity of messages sent and received.

1. Structured file in Edifact format

    - Structured file - MimeTypeQualifierCode: application/EDIFACT

2. Structured file in Cen BII or ISO20022 format

    - Structured file - MimeTypeQualifierCode: application/XML

Sub Mode	Document Identification/ Standard	ManifestItem/ MimeTypeQualifierCode	Additional Attachment	Signature Attachment
1	EDIFACT	application/EDIFACT	none	none
2	XML	application/xml	none	none

Mode 3: Business Control

This Mode is based on EU VAT directive implementation and instructions. In this mode the Sender and Receiver (Supplier and Buyer) are responsible to implement ”Business Controls”, including audit trails, to show authorities and auditors that their accounting, book-keeping etc. are based on actual business transactions of goods and services (order, delivery, invoicing and payments). The Sending Party and Receiving Party responsibility is to exchange the E-Invoice dataset and to do so in a manner that maintains the authenticity, integrity and legibility of the E-Invoice. The dataset is the”original”. An optional PDF view of the E-Invoice can be attached to the Structured File dataset.

1. Structured file in Edifact format

    - Structured file - MimeTypeQualifierCode: application/EDIFACT

2. Structured file in Cen BII or ISO20022 format

    - Structured file - MimeTypeQualifierCode: application/XML

Sub Mode	Document Identification/ Standard	ManifestItem/ MimeTypeQualifierCode	Additional Attachment	Signature Attachment
1	EDIFACT	application/EDIFACT	PDF (opt.)*	none
2	XML	application/xml	PDF (opt.)*	none

*PDF mime type (optional)

Format	ManifestItem/MimeTypeQualifierCode
PDF	application/PDF

EESPA
European E-invoicing Service Providers Association

Appendix 4 - EESPA RESPONSE MESSAGE V1.1

Transport Checks & Controls

1. Introduction

The EESPA Response Message provides e-Invoicing Service Providers with a single message that can be used to convey status details relating to invoice transmission, message validation and business processes.

This could readily extend to incorporate other document types, such as Purchase Orders, but is currently limited to invoice status information.

The structure of the EESPA Response Message provides a flexible information message that can be rapidly extended to meet business requirements of end user customer and service providers. EESPA will maintain and update the default status options. At the same time, the facility exists for users to include "local information" without the need to update the default qualifiers.

The three key uses of the EESPA Response Message are defined in the following three levels. However, within each level there will be multiple services that can be supported within the one message – such as payment status, query management and invoice financing.

Level 1 TRANSMISSION - Transfer Status (Technical Acknowledgement) as in AS2 protocol.

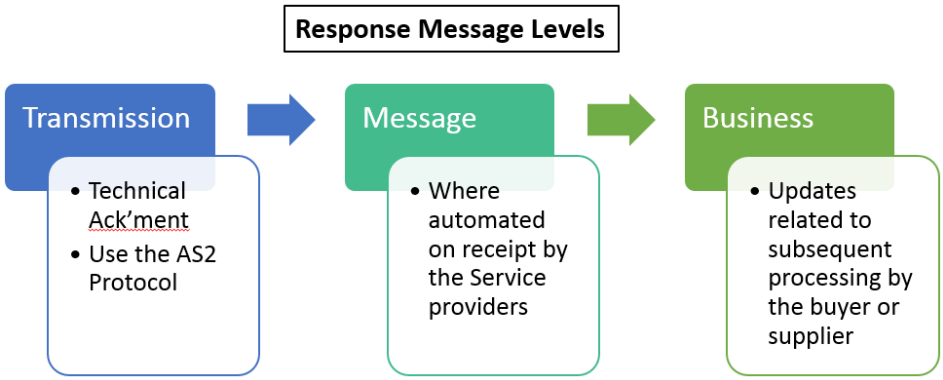
Level 2 MESSAGE - Status updates, related to Sending Party – Receiving Party Processing and which can be automated on receipt of the e-Invoice and are clearly defined and communicated within the Business Acknowledgement (response message)

2a. Legal compliance (EU Directive, Country and Industry)

2b. Business rules compliance undertaken by the SP for or on behalf of their Customer

Level 3 BUSINESS - Status updates, related to processing subsequent to the automated checks undertaken within Level 2 and related to the internal customer workflow process. These must also be clearly defined and communicated within the Business Acknowledgement (response message). Level 3 Status updates must be specifically agreed in advance between the Sending and Receiving Party if either Party is required to process this information in support of the Interoperability Services.

e.g. Customer status updates, such as invoice loaded into ERP or approved for payment.

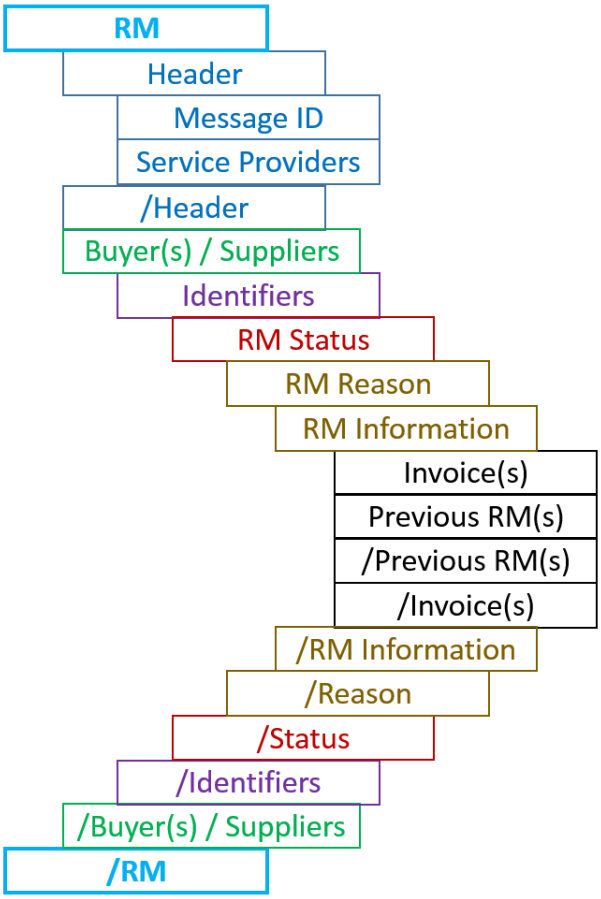


The Response Message is to allow for information normally only available within a 3-Corner model to be available where exchange is conducted using a 4-Corner Mode between Parties using the MIFA. This covers Message Level, Service Provider Level and Business Level response information. The Response Message is conveyed within the SBDH Envelope.

This provides the ability to exchange status information about any invoice at any time and the information conveyed principally falls within three categories:

- Transmission (RM1) Transfer Status
- Message Level (RM2) Status Information available from each Service Provider
- Business Level (RM3) Status changes and information following subsequent processing by the buyer or supplier

2. Structure of Response Messages



3. Definition of Response Messages

Each of the following definitions is based on the same Response Message Schema. The only difference is the information conveyed and the qualifiers used (as referenced in the section on Code Tables).

RM1 Transmission level status - Technical Acknowledgement

This is mandatory when using the MIFA.

However, as this is achieved using Message Delivery Notification (MDN) within AS2, duplication should be avoided by only using the Response Message for details that have NOT been covered successfully within the MDN.

RM1 is therefore not required as a separate message by use of the Response Message where this is provided by the MDN-AS2 acknowledgment.

4. RM2 Message level status updates - related to SP-SP Processing

These status updates relate to the SP-SP Processing which can be automated on receipt of the e-Invoice against the following sub-categories:

2a. Legal compliance (EU Directive, Country and Industry)

2b. Business rules compliance undertaken by the SP for or on behalf of their Customer

Mandatory RM2 Acknowledgements to be exchanged using the EESPA Response Message:

- where the invoice does not meet validation rules set by the Receiving Party and where the reason(s) for a rejection is(are) confirmed by the Receiving Party, with the rejection reason(s) to the Sending Party using this Response Message within no more than 24 hours from receipt of the Message.
    - This could result in an invoice being rejected (and not processed through to the Receiver).

5. RM3 Business level status updates

This is currently optional and to be agreed between the Parties to the MIFA.

This use of the response message corresponds to the exchange of business process information subsequent to the automated checks undertaken on receipt of the invoice and covered under RM2, between the buyer and the supplier. This will be dependent on this information being made available to the relevant SP. Where such information is available, this would be transmitted through the SP-SP interface. Examples would include confirming receipt, indicating that an invoice is in dispute or providing confirmation that an invoice has been cleared to be paid on a specific date.

6. Technical aspects

The following Schema defines the syntax to use for the exchange of Response Messages between Service Providers covering the wide range of different information requirements that can be conveyed.

The Schema Structure is outlined in Section 2. An XSD file and sample message are available if required.

The Response Message (RM) is able to reference invoices exchanged between one or more pairings of Sender and Receiver Companies with the response information section repeating as required. Similarly, each set of response information can be linked with one or more invoice.

A series of default qualifiers are provided (See sections 8, 9 and 10 below) to help Service Providers to establish a common understanding for the use of the Response Message. The Response Message has also been designed to allow Service Providers to agree additional qualifiers that can be used within the same Schema.

7. XML schemas of Response Messages

```
<ResponseMessage>
    <ResponseHeader>
        <RMID> Unique ID of the Response message </RMId>
        <RMTimestamp>ccyymmddhhmmss</RMTimestamp>
```

```
        <SPInformation>
            <SendingParty>
                <Id> ID for the Sending Service Provider </Id>
            </SendingParty>
            <ReceivingParty>
                <Id> ID for the Receiving Service Provider </Id>
            </ReceivingParty>
        </SPInformation>
</ResponseHeader>
<SenderReceiver>
        <Sender>
            <IdQualifier> type of Unique ID used (ex : DUNS, TVAintra) </ IdQualifier>
            <Id> Unique ID for the Sender Company </Id>
        </Sender>
        <Receiver>
            <IdQualifier> type of Unique ID used (ex : DUNS, TVAintra) </ IdQualifier>
            <Id> Unique ID for the Receiver Company </Id>
        </Receiver>
        <RMInformation>
            <RMStatus> see table below   </RMStatus>
            <RMReason> see table below </RMReason>
            <RMReasonDescription> description </RMReasonDescription>
            <RMInformationValue>
                <RMValueCode> See Table Below</RMValueCode>
                <RMValue> value relating to this Information </RMValue>
                <RMValueDescription> optional description to support the RMValue </RMValueDescription>
                <!—At least one of RMValueUoM or RMValueFormat to be included -->
                <RMValueUoM> Optional Unit of Measure relating to this Information </RMValueUoM>
                <RMValueFormat> Optional Format of this Information </RMValueFormat>
            </RMInformationValue>
            <InvoiceInformation>
                <!—Details for Invoice(s) covered by the RM Information  -->
                <InvoiceFilename> Option: The initial file name transmitted by SP-S </InvoiceFilename>
                <InvoiceFilenameDate> Option: ccyymmddhhmm </InvoiceFilenameDate>
                <InvoiceNumber> Invoice Number for this Invoice</InvoiceNumber>
                <InvoiceDate>ccyymmdd</InvoiceDate>
                <PreviousRM>
                    <PreviousRMID> Option: Previous RMID used for this Invoice </PreviousRMID>
                    <PreviousRMTimestamp>ccyymmddhhmmss</PreviousRMTimestamp>
                </PreviousRM>
            </InvoiceInformation>
        </RMInformation>
```

```
        </SenderReceiver>
</ResponseMessage>
```

8. Code tables

The code tables below are designed to provide a simple means of conveying specific status information and to do so within a clear data structure.

The high level structure of the code information is set out below and with the code lists in the tables that follow.

RMStatus

- RMS01000 Series = TRANSMISSION (Level 1)
- RMS02000 Series = MESSAGE (Level 2)
- RMS03000 Series = BUSINESS - Receiver Status (Level 3)
- RMS04000 Series = BUSINESS - Sender Status (Level 3)

RMReason

- RMR01000 Series = TRANSMISSION
- RMR02000 Series = MESSAGE
- RMR03000 Series = BUSINESS - For Receivers
- RMR04000 Series = BUSINESS - For Senders

Table for codes (XML segment: RMStatus)

STATUS	
Transmission	
RMS01000	Transfer Successful
RMS01100	Transfer Not Successful
RMS01200	Transmission Paused
Message	
RMS02000	Document rejected by SP-R
RMS02100	Document received and being processed by SP-R
RMS02150	Document under query by the Receiver
RMS02200	Document received and validated by SP-R
RMS02300	Document delivered by SP-R to Receiver
RMS02400	Document Corrupted – SP-R Unable to process
RMS02500	Document Awaiting Processing by SP-R
RMS02500	Document Awaiting Processing by SP-R
RMS02600	Document Approved
Business – Receiver Status	
RMS03000	Document Rejected by Receiver
RMS03100	Document acknowledged as received by Receiver
RMS03200	Document Under Query by Receiver
RMS03250	Document Under Dispute by the Receiver
RMS03300	Document awaiting matching / clearance to pay by Receiver
RMS03350	Document being processed by the Receiver
RMS03400	Invoice Cleared for Payment by Receiver
RMS03500	Invoice Paid by Receiver
RMS03600	Agreement to Early Settlement
RMS03700	Agreement to pass for invoice finance
RMS03750	Request for re-issue of a corrected invoice, without credit or credit note
RMS03800	Request for credit and credit note and the re-issue of a corrected invoice
RMS03900	Request for credit and credit note and no re-issued invoice
Business – Sender Status	
RMS04000	Document to be Credited by Sender
RMS04100	Document under review following query raised by the Sender
RMS04200	Document under review following query raised by the Receiver
RMS04300	Request for Early Settlement or other financing

RMS04400	Faulty goods / services
RMS04410	Late arrival preventing efficient use of the goods / services
Local Codes (where agreed)	
RMSLxxxx	"Local" option(s) defined as required (inclusion of "L" mandatory to protect the integrity of EESPA codes). "L" Local codes should be defined by SPs in bilateral relationships. "0" codes (i.e. where the first of the 5 final characters is a zero) are defined by EESPA and are not to be modified.

Notes:

- RMS02200 is an acknowledgement provided by the SP-R, when an invoice has been received and has passed agreed validation and/or legal compliance checks (e.g. mandatory fields checked, signature verified, etc.).
- RMS02300 corresponds to the acknowledgement provided by the SP-R, when an invoice (or invoice data) has been delivered to the buyer's information system. It does not prejudge the use that will be made by the buyer's information system. In case of pure outsourced e-invoicing services, it should correspond to the remittance of the e-invoice or the invoice data into the buyer's processing infrastructure.

Table for Reason codification (XML segment: RMReason)

REASON	
Transmission Reasons	
RMR01000	Transfer timed out
RMR01100	Transfer error – Unable to re-attempt transfer process
RMR01200	Transfer error – Will re-attempt transfer process
Message Reasons	
RMR02100	Unable to extract required data from Invoice
RMR02200	PO Reference not found
RMR02210	PO Reference not valid
RMR02250	GRN Reference not found
RMR02260	GRN Reference not valid
RMR02300	VAT Reference not found
RMR02400	Error found in invoice line, VAT or Total values
RMR02500	Currency not supported
RMR02600	Unknown Receiver
RMR02700	PDF representation of the invoice was not provided
Business (Receiver) Reasons	

RMR03000	Faulty goods / services
RMR03100	Late arrival preventing efficient use of the goods / services
RMR03200	Contract no longer valid.
RMR03300	Commercial transaction not recognised
RMR03310	Prices not according to contract or quotation
RMR03320	Quantity not according to delivery
RMR03330	Delivered quantity exceeding approval or order
RMR03340	Payment terms are not as agreed
RMRLxxxx	"Local" option(s) defined as required (inclusion of "L" mandatory to protect the integrity of EESPA codes) "L" Local codes should be defined by SPs in bilateral relationships. "0" codes (i.e. where the first of the 5 final characters is a zero) are defined by EESPA and are not to be modified.
Business (Sender) Reasons	
RMR04000	Invoice to be credited and re-issued
RMR04100	Invoice to be credited and not re-issued
RMRLxxxx	"Local" option(s) defined as required (inclusion of "L" mandatory to protect the integrity of EESPA codes) "L" Local codes should be defined by SPs in bilateral relationships. "0" codes (i.e. where the first of the 5 final characters is a zero) are defined by EESPA and are not to be modified.

Table for Response Message Information Value (XML segment: RMValueCode)

This table could precise or complete “sub-codification” of RMReason.

RMI0010	Date/Time Next Attempt will be made to process the invoice(s)
RMI0020	Date Invoice Status Changed to “Under Query”
RMI0030	Date Invoice Query Status Changed to become ‘OK To Process’
RMI0040	Date when payment will be made
RMI0050	Date the payment was made
RMILxxx	“Local” option(s) defined as required (inclusion of “L” mandatory to protect the integrity of EESPA codes) “L” Local codes should be defined by SPs in bilateral relationships. “0” codes (i.e. where the first of the 5 final characters is a zero) are defined by EESPA and are not to be modified.

Appendix 5 - Addressing and Routing Protocol

1. Introduction

This appendix defines the Addressing & Routing protocol that can be used between Parties to the MIA. This is mandated as part of the EESPA Multilateral Interoperability Framework Agreement (MIFA) but is optional under the MIA.

This appendix describes a uniform standard for identifying each Customer (Buyer or Supplier) as well as the Service Provider to which each is connected.

To enable interoperability for a large number of entities a highly automated process is required.

This Protocol defines an approach that can be used between two EESPA Members in conjunction with the EESPA MIA.

This approach includes an "Addressing ID" for each Customer (Sender and Receiver) and a "Routing ID" (the EESPA Routing ID's (ERID's) - for each of the Service Providers.

The EESPA "Routing ID" (ERID) is managed and assigned by EESPA to its members.

The Addressing ID is defined by each Service Provider for or on behalf of its Customer and MUST be unique within their customer-base.

The combination of the Routing and Addressing ID's is therefore Globally Unique.

2. EESPA Routing ID (ERID)

The ERID Routing ID is a distinctive code that serves to identify the Sending Party and the Receiving Party when Messages are to be routed between two EESPA Service Providers. Such an ID is required where the Sender and Receiver are connected to different Service Providers. The ERID can be used as part of the Transport Protocol and the Message to identify the two Service Providers – i.e. the Sending Party and the Receiving Party.

The EESPA Routing ID's for all EESPA Members are defined, maintained and issued by EESPA in support of this Protocol.

3. Routing ID syntax

The EESPA Routing ID consists of the following three components:

(i) EESPA Routing Identification (provided by EESPA). [an7]

(ii) Optional divider "/" included ONLY where the following "Sub-Identification" is required.

(iii) Optional Service Provider Routing "Sub-Identification". [an2]

NOTES:

(a) Sub-Identifications, where required, must also be defined, maintained and issued by EESPA in support of this Protocol.

(b) This "Sub-Identification" should ONLY be used where required to manage the technical routing of the Message.

Name	Data Type	Length	Format	Description
Sending Party Routing ID (ERID)	Alpha Numeric	10	an7/an2	Unique Identifier for the Sending Service Provider
Receiving Party Routing ID (ERID)	Alpha Numeric	10	an7/an2	Unique Identifier for the Receiving Service Provider
Examples: **E123456/FI** **E0017621** **E0000124/BE**				

4. Issuing Routing ID's (ERID's)

The EESPA´s Executive Committee will manage the provision of Unique Routing ID's, and Sub-Identifications where required, to each Service Provider. Each member would be notified of its unique EESPA Routing ID upon being admitted as a member of EESPA. EESPA Routing IDs would remain the property of EESPA and be maintained within a central EESPA register. Each Member is able to request one or more Sub-Identifications where these are required.

5. Addressing ID (Customer ID)

A second identifier is used for each of the Customers and is required for both the Sender and Receiver. This is known as the Addressing ID.

Each Service Provider is free to assign any Addressing ID to its own customers.

Depending on the business operating structure, a company may only need a single addressing ID or may need multiple Addressing ID's for each trading company, sub-company or division.

An Addressing ID is required for each trading entity from or to which E-Invoices or Electronic Business Documents are to be routed and is allocated by the Service Provider for each of its own trading parties.

To be able to cover different standards already in use, this number is alphanumeric and has no limit in the number of characters.

Where a specific Addressing ID type is used (e.g. a VAT Number) then a qualifier can be included within the Message to describe the specific type in use.

Name	Data Type	Length	Authority Qualifiers (Optional)	Description
Addressing ID	Alpha Numeric	unbounded	"EAN.UCC" = The ID is a GLN "VATIN" = The ID is a VAT Number "EESPA" = The ID is an EESPA defined reference for the Customer "COUNTRYCODE:ORGANISATIONIDENTIFIER" = Country Code (ISO 2 Digit) & Organisation ID (e.g. DE54223332) "NONE" = No qualifier provided for this ID Others could be agreed by the Parties and defined within the Description of Services.	Unique Identifier for either Customer (Sender or Receiver)
Examples: **GB12265338290** **(Qualifier = VATIN)** **503837725414253** **(Qualifier = EAN.UCC)** **554FRT7723311** **(Qualifier = NONE)**				

6. Globally Unique ID

The combination of the EESPA Routing ID and the Addressing ID (defined by each Service Provider for or on behalf of its Customer and unique within their customer-base) provides an ID's that is Globally Unique and therefore able to be used to support multilateral exchange.