UNITED NATIONS

E

Economic and Social Council

Distr.
GENERAL

TRADE/CEFACT/2003/19
27 February 2003

ENGLISH ONLY

ECONOMIC COMMISSION FOR EUROPE

COMMITTEE FOR TRADE, INDUSTRY AND ENTERPRISE DEVELOPMENT

Centre for Trade Facilitation and Electronic Business (UN/CEFACT)

Item 6 of the provisional agenda

Ninth session, 12 – 13 May 2003

Trading Partner Agreement

"General Legal Provisions"
"Non-Disclosure Agreement"
"Appendix for Portal Services"
"Appendix for XML Services"
"Appendix for EDI Services"

Submitted by RosettaNet, EDIFICE, ESIA/EECA and UN/CEFACT*

* The present document is submitted in the form in which it was received by the secretariat.

TRADING PARTNER AGREEMENT - General Legal Provisions

1. Effective Date

The effective date of this Trading Partner Agreement is: ______________________________________.

2. Parties

This Trading Partner Agreement (hereinafter the "Agreement") is entered into by and between:

____________________________*(Company name)*, a company incorporated in ____________________
_____________________________ *(Country/State)* and organised and existing under the laws of ____
__ (*Country/State)*, having its principal place of business at ____
____
(Address)

(hereinafter "______________________", or Party),

and

____________________________*(Company name)*, a company incorporated in ____________________
_____________________________ *(Country/State)* and organised and existing under the laws of ____
__ (*Country/State)*, having its principal place of business at ____
____
(Address)

(hereinafter "______________________", or Party).

Hereinafter collectively referred to as the Parties.

3. Definition of Terms

Adopted Format: The accepted method for the Electronic Information Exchange according to the applicable Specifications and Appendices, or such other format that may be agreed in writing by the Parties.

Confirmation of Acceptance: Electronic Information returned to a requesting Party to confirm the business acceptance of a request.

Confirmation of Receipt: Electronic Information returned to a requesting Party to confirm the business receipt of a request.

Data Log: The Data Log is the complete Record of data interchanged between the Parties.

Digital Signature: A Digital Signature is an Electronic Signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

Electronic Information Exchange: Means of Electronic Commerce defined to include, but not limited to, the exchange of messages, documents and data using Information exchange technologies like Electronic Data Interchange, Facsimile, Electronic

Mail, and Internet-based Transactions making use of Extensible Markup Language and Portal technology.

Electronic Signature: An Electronic Signature means an electronic sound, code, symbol, or process, attached to or logically associated with a contract or other document and executed or adopted by a person with the intent to sign the document.

Encryption: Encryption is the conversion of data by means of mathematical algorithms into a form (secret code) that cannot be easily understood by unauthorized people.

Information: Information means data, text, images, sounds, codes, computer programs, software, databases, or the like.

Record: Record means Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Service: A Service is a software module deployed on network accessible platforms provided by the Service Provider. Its interface is described by a Service description. It exists to be invoked by or to interact with a Service requestor. It may also function as a requestor, using other Services in its implementation.

Service Provider: A company that provides to its Trading Partner Electronic Information Exchange Services that would otherwise have to be located in their own company computers. The Service Provider is the owner of the Services offered.

Specifications: The set of standards, protocols and documents describing business and technical procedures and rules and other requirements applicable to the Electronic Information Exchange agreed using the Adopted Format identified in the Appendices to this Agreement.

Trading Partner: A company using Electronic Information Exchanges under this Agreement.

Transaction: A Transaction means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more Trading Partners, including any of the following types of conduct: (a) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) Services, and (iii) any combination thereof; and (b) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

4. Object and Scope

These provisions shall govern the terms and conditions of the Agreement between the Parties in respect to the exchange and processing of Information by electronically transmitting and receiving data with the Adopted Format.

Because the Parties have agreed to use Electronic Information Exchange as a substitution for conventional paper-based documents, this Agreement is to ensure that such Transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the Parties.

The Parties agree that any portion of this Agreement which aims to determine contract formation or otherwise change, cancel or modify any other legal rights or remedies (a) is inapplicable; (b) does not form a part of this or any other Agreement between the Parties; (c) does not create any agency, partnership, joint venture relationship or other business relationship between the Parties.

5. General Terms and Conditions

This Agreement adopts and incorporates by reference all of the terms and conditions of the ___________________________ *(title of the referenced contracts / documents)* signed between the Parties dated as of ______________ *(effective dates)* and attached hereto as _____________________ *(name of the attachments)* and all of its Annexes. The terms and conditions of this Agreement shall only prevail in the event of any conflict related to electronic Transactions.

Each Party represents and warrants that (a) it has obtained all necessary approvals, consents, and authorizations of third Parties and governmental authorities to enter into this Agreement and to perform and carry out its obligations hereunder; (b) the persons executing this Agreement on its behalf have express authority to do so, and in so doing, to bind the Party thereto; and (c) this Agreement is a valid and binding obligation of such Party, enforceable in accordance with its terms.

Except as expressly stated above or otherwise specifically agreed neither Party makes any representation or warranties and each Party hereby expressly disclaims all representations and warranties express or implied related to this Agreement.

This Agreement shall not be assigned or transferred by either Party without the prior written consent of the other Party.

6. Recording and Storage

All Electronic Information shall be transmitted in a form that is capable of being recorded, stored and accurately reproduced for later reference by all the Parties.

The Records of the Information exchanged electronically will be stored unaltered and securely in order to maintain trade Data Log of all transmissions as they were sent and received, in accordance with the time limits and Specifications prescribed by legislative requirements that may apply in either of the respective countries of the Parties, and, in any event, for a period of _____ (__) years unless otherwise specified in the applicable Appendix.

Each Party shall comply with all relevant local and national laws or regulations relating to the data protection, and in particular shall maintain and use any personal data it may have access to in the course of the business relationship exclusively for the intended purpose.

7. Confidentiality and Third Party

Unless otherwise specifically agreed, all Electronic Information transmitted hereunder, and the electronic and Digital Signatures used as security measures for the exchanges, shall be deemed the confidential property of the originating Party, covered by and subject to the terms of the Non-Disclosure Agreement between the Parties.

Electronic Information may be exchanged either directly or through a Service Provider with whom either Party may contract. The Party contracting with a Service Provider must require that such Service Provider use confidential Information disclosed to or learned by such Service Provider only in connection with providing Services in accordance with an agreement signed by such Service Provider containing terms no less protective of such confidential Information than the terms of the Non-Disclosure Agreement between the Parties.

Either Party may modify its election to use or may change a Service Provider upon 30 days prior written notice to the other Party.

8. Security

Each Party shall properly implement the security procedures and infrastructure detailed in the applicable Specifications and Appendices, or if security procedures are not specified, shall properly implement security procedures that are sufficient to ensure that all Information exchanges are authorized and secure and to protect the Information transmitted, its business Records, and data from improper access and use, alteration, false denial, destruction, or loss.

For all Electronic Information Exchanges requiring Encryption as specified in the applicable Specifications and Appendices, each Party shall encrypt the Information accordingly.

Each Party shall comply with all local and international regulations related to the import, export and use of cryptographic products. As several countries have restrictions on such products, and their laws tightly control their use, each Party shall agree to comply with applicable laws governing the obligation to obtain a license for export, import or industrial use of any cryptographic product in the country in which such requirements are in effect.

9. Electronic Signatures

In order to exchange Electronic Information, each Party shall adopt an Electronic Signature, which shall be affixed to or contained in each message transmitted by such Party. Each Party agrees that any Electronic Signature of a Party affixed to or contained in any transmitted message shall be deemed signed, duly given, and legally sufficient to verify that said Party originated the message.

The Parties agree that the exchange of Information pursuant to the applicable Specifications and Appendices will create valid and enforceable obligations, which will, in all respects other than the means of their transmission and receipt, be governed by the terms and conditions of the applicable agreements between the Parties.

Where particular Specifications require that the receiving Party issue a notice to the other confirming receipt, such notice will not constitute a binding acceptance or confirmation of anything more than mere receipt.

Any message or document properly signed to which is affixed a valid Electronic Signature and transmitted pursuant to this Agreement, or in connection with any Transaction or any other agreement described in Section 5, shall be considered to be a "writing" or "in writing" and to constitute an "original" when printed from electronic files or Records established and maintained in the normal course of business, admissible as between the Parties in a forum of any competent judicial, arbitration, mediation, or administrative proceeding to the same extent and under the same conditions as any other business Records originated and maintained in documentary form.

The Parties agree not to contest the validity or enforceability of signed documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the Party to be bound thereby.

10. Digital Signatures

For each document, for which a Digital Signature is required to be used as the Electronic Signature as specified in the applicable Specifications or Appendices, each Party shall digitally sign such documents prior to transmitting them to the other Party. Each Party shall verify the authenticity and integrity of each such digitally signed documents that it receives from the other Party, according to the Digital Signature infrastructure detailed in the applicable Appendix.

11. Processing

Information exchanged electronically shall not be deemed to have been properly received, and no document shall give rise to any obligation, until accessible to the receiving Party at such Party's receipt computer designated in the applicable Appendices.

Upon proper receipt of any Electronic Information, the receiving Party shall promptly and properly transmit a Confirmation of Receipt in return, unless otherwise specified in the corresponding Appendix. The Confirmation of Receipt shall constitute conclusive evidence that the Electronic Information has been properly received.

If the receiving Party is obliged to provide a Confirmation of Receipt and the confirmation has not been received by the sender as specified in the applicable Specification or Appendix, the sender: (a) may give notice to the receiver stating that no confirmation has been received and specifying a reasonable time by which the confirmation must be received; and (b) if the confirmation is not received within the time specified in (a) above may, upon notice to the addressee, treat the Information exchanged as though it had never been sent, or exercise any other rights the sender may have.

Any Electronic Information, which has been properly received, shall not give rise to any obligations unless and until the Party initially transmitting such Information has properly received in return a Confirmation of Acceptance, where required, as specified in the applicable Appendix.

If any transmitted Information is received erroneously, or in an unintelligible, or corrupted, or duplicated form, the receiving Party shall promptly notify the originating Party (if identifiable from the received Information) in a timely manner. In the absence of such a notice, the originating Party's Record of the contents of such transmitted Information shall control.

12. Operational Requirements

Each Party shall use all commercially reasonable efforts to (a) provide, maintain and test its respective equipment, software, security procedures and Services as necessary to effectively, reliably and securely transmit and receive Electronic Information, and (b) to provide sufficient notice to the other of any changes in systems operations, hardware or software that might impair the mutual capabilities of the Parties to communicate in accordance with the applicable Specifications and Appendices.

Each Party shall bear all of its own costs associated with (a) the implementation, maintenance and use of these Specifications; (b) any Service Provider with which each Party may contract.

13. Liability

No Party shall be liable for any failure to perform its obligations in connection with any Transaction or any Information exchanged, where such failure results from any act of nature or other cause beyond such Party's reasonable control, including without limitation, any mechanical, electronic or communications failure, which prevents such Party from electronically transmitting or receiving any Information.

Neither Party shall be liable to the other for any indirect, special, incidental, exemplary or consequential damages arising from or as a result of any delay, omission or error in the electronic transmission or receipt of any Electronic Information pursuant to this Agreement, even if the Party has been advised of the possibility of such damages.

Each Party shall be liable for direct damages originated by the acts or omissions of its Service Provider while transmitting, receiving, storing, or handling Electronic Information, or performing related activities for such Party. If both Parties use the same Service Provider to exchange the Electronic Information, the originating Party shall be liable for the acts or omissions of such Service Provider as to such exchanged Information.

Each Party shall be responsible for the costs of any Service Provider with which it contracts, unless otherwise set forth in an Appendix.

14. Applicable Law

This Agreement shall be construed and interpreted in accordance with the laws of ____________________ (*Country/State*), without prejudice to any mandatory legislative provision, which may apply to the Parties with regard to processing, recording and storage of Electronic Information, or confidentiality and protection of personal data.

15. Termination

This Agreement shall remain in effect until terminated by either Party with not less than 30 days prior written notice, which notice shall specify the effective date of termination; provided, however, that any termination shall not affect the respective obligations or rights of the Parties arising under any exchanged Information or otherwise under this Agreement and any other agreement signed between the Parties prior to the effective date of termination. Those provisions that by their nature are continuing obligations shall survive any termination and remain binding upon the Parties.

16. Severability

Any provisions of this Agreement, which are determined to be invalid or unenforceable, will be ineffective to the limited extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

17. Entire Agreement

This Agreement and the Appendices (____________ _____________________________, Version _______,
effective date _______________; _______________ _____________________________, Version _______,
effective date ________________; _______________ _____________________________, Version _______, effective date _________________) constitute the complete Agreement of the Parties relating to the matters specified in this Agreement and supersede all prior representations or agreements, whether oral or written, with respect to such matters.

No modification or waiver of any of the provisions of this Agreement shall be binding on either Party unless made in a paper-based writing and signed by an authorized representative of each. No obligation to enter into any Transaction or any further contractual relationship is to be implied from the execution or delivery of this Agreement.

This Agreement is for the benefit of, and shall be binding upon, the Parties and their respective successors and assigns.

This Agreement may be translated into other languages, but the English language version will be the official version and will control the construction and interpretation hereof.

IN WITNESS WHEREOF, the Parties hereto execute this Agreement.

-- (Company name)

Signature:

____

Typed Name: ___________________________

Title: ___________________________________

Date/Place: _____________________________

-- (Company name)

Signature:

____

Typed Name: ___________________________

Title: ___________________________________

Date/Place: _____________________________

TRADING PARTNER AGREEMENT – Non Disclosure Agreement

1. Effective Date

The effective date of this Non-Disclosure Agreement is: ___________________.

2. Parties

This Non-Disclosure Agreement (hereinafter the "Agreement") is entered into by and between:

_____________________________*(Company name)*, a company incorporated in _____________________
______________________________ *(Country/State)* and organised and existing under the laws of ____
__ *(Country/State)*, having its principal place of business at ____
____
(Address)

(hereinafter "_______________________", or Party),

and

_____________________________*(Company name)*, a company incorporated in _____________________
______________________________ *(Country/State)* and organised and existing under the laws of ____
__ *(Country/State)*, having its principal place of business at ____
____
(Address)

(hereinafter "_______________________", or Party).

Hereinafter collectively referred to as the Parties.

3. Purpose

Whereas the Parties may disclose proprietary and Confidential Information by exchanging Information electronically for the purpose of evaluating the feasibility and modality of possible business relationship between the Parties and for the purpose of the possible business relationship which is a consequence of said evaluation (hereinafter the "Purpose").

4. Definition of Confidential Information

Confidential Information under this Agreement shall mean any technical and commercial information relating to respective businesses of each Party or Affiliates, including but not limited to facilities, products, documentations, specifications, know-how, techniques and processes and other information pertaining to the business relationship, which is disclosed by one Party (hereinafter referred to as the "Discloser") to the receiving Party (hereinafter referred to as the "Recipient") under this Agreement whether in form of oral and visual disclosure, in writing, in graphic, electronic, or electromagnetic form and any derivatives of any of the foregoing.

5. Use of Confidential Information

The Parties agree that all Confidential Information disclosed hereunder in whatever form shall (a) not be used for any purpose other than the above-mentioned Purpose; (b) not be disclosed to third Parties without the prior written permission of the Discloser; (c) be kept as strictly confidential; (d) remain the property of the Discloser and shall not be copied or reproduced without the express written permission of the Discloser, except for such copies as may be absolutely necessary in order to perform the evaluation contemplated hereunder.

Upon expiration or termination of this Agreement, or within ____ (__) days of receipt of Discloser's written request, Recipient shall return all Confidential Information to Discloser along with all copies and portions thereof, or certify in writing that all such Confidential Information has been destroyed.

6. Protection of Confidential Information

A Recipient shall protect the disclosed Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the Recipient uses to protect its own Confidential Information of a like nature.

1.Each Recipient undertakes to restrict the use, the further disclosure and the access to Confidential Information to only those of its employees, to whom such access is necessary for carrying out the Purpose and advise such employees of the obligations assumed herein.

2.The Recipient shall have a duty to protect only that Confidential Information which is (a) marked or identified as confidential or with similar identification(s) at the time of disclosure, or which is (b) disclosed by the Discloser in any other manner, e.g. orally, and is confirmed in writing as being confidential by the Discloser within thirty (30) days after the disclosure.

[1] This provision may be adapted depending on the Company's legal model.

[2] This provision may be adapted depending on the Company's legal model.

7. Exclusions

This Agreement imposes no obligation upon a Recipient with respect to the Confidential Information which (a) was in the Recipient's possession before receipt from the Discloser; (b) is or becomes a matter of public knowledge through no fault of the Recipient; (c) is rightfully received by the Recipient from a third Party without a duty of confidentiality; (d) is disclosed by the Discloser to a third Party without a duty of confidentiality on the third Party; (e) is independently developed by the Recipient without the use of any of the Discloser's Confidential Information or any breach of this Agreement; (f) is disclosed under operation of law; or (g) is disclosed by the Recipient with the Discloser's prior written approval.

8. Affiliates

The Parties agree that (a) they both may disclose Confidential Information to their Affiliates but only to the extent that such Affiliates have a need to know for the purpose of carrying out the Purpose; (b) disclosure by or to an Affiliate of a Party hereto shall be deemed to be a disclosure by or to that Party and shall be governed by this Agreement, as applicable; (c) the employees of the Affiliates shall comply with the terms and conditions of this Agreement.

3Each Party's disclosures to its Affiliates shall be (a) defined under this Agreement before any Confidential Information is disclosed; and (b) limited to those Affiliates which are listed in section 16. The Parties agree that in case of any change regarding these lists each Party shall notify the other immediately, and that updates of these lists will be allowed only if duly authorized by both Parties.

For the purposes of this Agreement "Affiliate" shall mean any corporation, partnership, or other entity which, directly or indirectly, owns, is owned by, or is under common ownership with, such Party hereto, for so long as such ownership exists, and as long as at least fifty per cent (50%) of the outstanding shares, or securities, or other equity interests entitled to vote for the election of directors or other managing authority or governing body.

9. Proprietary Rights

Neither Party (a) acquires any intellectual property rights nor any other rights under this Agreement except the limited right to use set out in section 5 above; (b) is entitled to assign or transfer any of its rights, benefits and obligations under this Agreement without the prior written consent of the other Party.

10. Disclosure Period

This Agreement shall remain in force for a period of ____ (_) year(s) as from the Effective Date. However, either Party may terminate this Agreement on _____ days (__) written notice to the other, prior to its expiry.

The obligations linked to the confidentiality contained in this Agreement shall bind the Parties for a period of _____ (_) years from the date of disclosure of Confidential Information, regardless of termination or earlier expiration of this Agreement.

11. Export Administration

Each Party agrees to comply fully with all relevant export control laws that may apply to assure that (a) no Confidential Information or any portion thereof with respect to products and services is exported, directly or indirectly, in violation of the laws and applicable regulations of the country in which the Parties reside; (b) no Confidential Information will be used for any purpose prohibited by the laws that may apply including, without limitation, nuclear, chemical, or biological weapons proliferation.

12. Dispute Resolution

4A choice is to be made by the Parties between the two alternatives Arbitration clause and Jurisdiction clause.

Arbitration clause

Any dispute arising out of or in connection with this Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration. The arbitrator is to be nominated by ____________________ (*Appointing authority*), in accordance with and subject to the rules or procedure of __________________________. The arbitration shall be held in ________________________ (*Country/State*).

Jurisdiction clause

Any dispute arising out of or in connection with this Agreement shall be referred to the courts of ______________________ (*Country/State*), which shall have sole jurisdiction. However, a Party shall furthermore have the right to sue the other Party in the courts at the other Party's domicile.

13. Applicable Law

This Agreement shall be construed and interpreted in accordance with the laws of _____________________ (*Country/State*), excluding its rules for choice of law.

14. Entire Agreement

This Agreement sets forth the entire Agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements, representations, communications or understandings concerning such

[3] This provision may be adapted or deleted depending on the Company's structure.

[4] This provision may be adopted or deleted depending on the Company's legal model.

Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both Parties.

15. Miscellaneous

Neither this Agreement nor disclosure or receipt of Confidential Information shall constitute or imply any promise or intention to make any purchase of products or services by either Party or any additional commitment, right or obligation by either Party with respect to the present or future marketing of any product or service or any promise, intention or obligation to enter into any other business arrangement of any kind.

All Confidential Information disclosed hereunder shall be provided by Discloser without representation or warranty of any kind.

Nothing in this Agreement shall be deemed to grant either Party a license directly or by implication under any patent, patent applications, trademark, copyright, design right (whether registrable or not) mask work rights, trade secrets, know-how or any other intellectual property right.

16. List of the Affiliates

5_________________'s *(Company A)* Affiliates:

-

-

-

-

-

-

_________________'s *(Company B)* Affiliates:

-

-

-

-

-

-

IN WITNESS WHEREOF, the Parties hereto execute this Agreement.

-------------------------------------- (Company name)

Signature:

____

Typed Name: __________________________

Title: _________________________________

Date/Place: _____________________________

-------------------------------------- (Company name)

Signature: ______________________

Typed Name: __________________________

Title: _________________________________

Date/Place: _____________________________

[5] This provision may be adopted or deleted depending on the Company's legal model and on the business purpose.

Appendix 1: TPA Module for Portal Services

The objectives of this Appendix are: (a) To emphasize the obligations of the Parties to the Trading Partner Agreement (hereinafter "Agreement") in accessing and using _______________’s *(Company A)* collaborative Portal (“*Portal Name*”), in particular the obligations to monitor and announce in a timely manner any change about Users and their rights and privileges to see or add content, and to use applications in a personalized environment of the collaborative Portal; (b) To identify the Parties and define the technical means related to the use of the collaborative Portal.

1.1. Portal Business Specifications

The Parties agree to cooperate to ensure that only ____________________’s (*Company B*) Users mutually approved by the respective Portal Authority have the right to use the Portal Services agreed.

The Parties agree that the Portal Authorities shall collaborate to monitor the current access list of names of those Users who are allowed to access and use collaborative Portal Services. In case of any change regarding the User’s access list and rights, the Portal Authority responsible for the change shall inform the other in a timely manner.

The Parties agree that ____________ (*Company A*) has the right to (a) add/remove a User to/from the access list; (b) update the access list whenever an event affects it, including, but not limited to, activation, revocation or changes in User’s access rights, privileges and User’s Profiles for the use of a Portal Service; (c) modify, delete, exchange and validate User’s attributes recorded in an Enterprise Directory; (d) refuse access to specific, individual Users.

Where clarifications should be required as due to a dispute event, the Parties agree that ____________ (*Company A*) will limit the use of the Portal for the User(s) concerned with the dispute to a suitable environment with restricted rights, until dispute resolution is reached.

The Parties agree that by accessing the Portal for the first time each User (a) shall agree with and shall be bound by the *Terms of Use*, which governs the use of the Portal; (b) shall accept to provide personal User's Information that may be collected and used for the purpose of furthering the business relationship between the Parties to the Agreement.

This Appendix is governed by the general legal provisions of the Trading Partner Agreement, Version _____, effective date __________________.

This Appendix, and the Trading Partner Agreement, may be considered as a part of another related agreement: _______________________________________ (*title of the related agreement*), effective date __________________.

1.2 Portal Technical Specifications

Parties to the Agreement	Company Name	Company Representative	Effective Date
Company A			
Service Provider A			
Company B			
Service Provider B			

Company A		
IDENTIFICATION	Company Address:	
	DUNS Number(s):	
	Contact Person for Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Portal Authority	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider	Name: Address: Responsible: Tel.: Fax: Email:
	Authorized IP Addresses:	

Company B		
IDENTIFICATION	Company Address:	
	DUNS Number(s):	
	Contact Person for Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Portal Authority	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider	Name: Address: Responsible: Tel.: Fax: Email:
	Authorized IP Addresses:	

PORTAL SERVICE 1		
	Application	Name: ………………………. Specification: …………………….. Note: A definition of the Application can be included in the Glossary.
	Portal URL:	https://………..
	Password Creation and Management	Procedure: ………………………. e.g. User changes password in full privacy by operating a self-registration to create the User's account prior to any Service-specific configuration.
	Content Visibility	Description: ………………………. e.g. Personalized content according to User Profile; customized centre of interest; search engine; etc.
	Content Contribution	Description: ……………………….. e.g. Publish documents in a private environment; classification of documents; choice of content viewers; etc.) Note: Anti-Virus Check before posting content is mandatory!
	Security	Requirements: e.g.: • Anti-Virus Check before posting any content to the Portal • Browser version supporting SSL Encryption with Cipher Strength 128 bits • Non-repudiation of origin and content;
		Procedures: …………………….. e.g. Authentication, Authorization, User's profiling, secure Protocol, IP Filtering, Cryptography methods of Encryption and Digital Certificate validation, etc.
		Infrastructure: …………………….. e.g. Firewall, Anti-Virus, Smart Card, VPN, etc.
		Other Specifications: ……………………….
	Failure Procedures	Requirements / Specifications: e.g. Inform the other Party within ___H; request to retry or retry the transmission of Information immediately; 3 d for processing Authorization request, if failure then + 3 d for processing, if failure then change rights/privileges, new request submission; etc.
	Service Availability	Specification: ………………………. e.g. ___%;
	Service Level Support	Specification: ………………………. e.g. 1st level: 7x___H support via Portal Authority and Portal form/email, etc.

1.3. Glossary

Anti-Virus: The Anti-Virus is software - a class of program that searches the hard drive and floppy disks for any known or potential electronic viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their Information and computer assets.

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), Authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the User is authentic. The use of Digital Certificates issued and verified by a CA as part of a Public Key Infrastructure is considered likely to become the standard way to perform Authentication on the Internet.

Authorization: Authorization is the process of giving Users permission to use a computer operating system or an application by defining which Users are allowed access to the system and what privileges of use apply. Assuming that someone has logged in to a computer operating system, the system or application may want to identify what resources the User can be given during this session. Thus, Authorization is sometimes seen as both the preliminary setting up of permissions by a system adminstrator and the actual checking of the permission values that have been set up when a User is getting access. Logically, Authorization is preceded by Authentication.

Certificate Authority: A Certificate Authority (“CA”) is an authority in a network that issues and manages security credentials and Public Key for message Encryption. A CA associates Digital Certificates with a specific person or entity, identifies the person or entity that is to receive a Digital Certificate, issues and revokes these when required, and provides notice of revocations in a published Certificate revocation list.

Cipher: A Cipher is any method of encrypting text. It is also sometimes used to refer to the encrypted text message itself.

Cryptography: Cryptography is the science of Information security. Modern Cryptography concerns itself with the following four objectives: (a) Confidentiality (the Information cannot be understood by anyone for whom it was unintended); (b) Integrity (the Information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected); (c) Non-repudiation (the creator/sender of the Information cannot deny at a later stage his or her intentions in the creation or transmission of the Information); (d) Authentication (the sender and receiver can confirm each others identity and the origin/destination of the Information).

Digital Certificate: A Digital Certificate (in short: “Certificate”) is an electronic identification containing the credentials to operate business transactions via Internet. A Certificate is issued by a CA and contains the owner’s name, a serial number, the expiration dates, a copy of the Certificate Public Key, which is used for Encryption and Digital Signature, and the Digital Signature of that Certificate Authority to allow a recipient for verification of Certificate validity.

Digital Signature: A Digital Signature is an Electronic Signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

DUNS ® Number: The Data Universal Numbering System (“DUNS”) is a sequentially generated nine-digit number that is assigned and maintained only by Dun and Bradstreet (http://www.dnb.com), which identifies unique business locations, and is global in scope.

Encryption: Encryption is the conversion of data by means of mathematical algorithms into a form (secret code) that cannot be easily understood by unauthorized people.

Enterprise Directory: In computer networks, an Enterprise Directory is a repository collecting attributes of resources. For instance, attributes may concern employees (User names, passwords, job specifications, etc.) and network/computing resources (IP Addresses, cost centers, computers, etc.).

Firewall: A Firewall is a set of related programs that protects the resources of a private network from Users from other networks, and it is often installed in a specially designated computer separate from the rest of the network. An enterprise with an intranet that allows its employes access to the wider Internet installs a Firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own Users have access to.

IP Address: The Internet Protocol (in short: “IP”) is the method or Protocol by which Information and data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP Address that uniquely identifies it from all other computers on the Internet. When Information is transmitted, the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address.

IP (Address) Filtering: Controlling access to a network by analysing the incoming and outgoing packets and letting them pass or halting them based on the IP Addresses of the source and destination. Packet filtering is one technique, among many, for implementing security Firewalls.

Portal: A Portal is a Web site that serves as a single gateway to a company's Information and knowledge base for employees and possibly for Customers, business Partners, and the general public as well. In one model, it contains a set of Information - content areas, pages, applications, and even data from outside sources - brought together in one central location and accessed and used through a common interface. This interface is a page being the face of the Portal: what Users see and use to interact with the content of the Portal.

Portal Administrator: A personal assigned by ___________________ (*Company A*), whose task includes, but is not limited to, granting security and creating passwords following the ____________________ (*Company A*) certified Users management procedure.

Portal Authority: The Portal Authority is the contact person within a Party's organization that is responsible of managing the Portal's use with the other Party. The Portal Authority drives the activities related to the definition of User's access to Portal Services, and are enabled to recognize a User as compliant for using a specific, personalized environment of the Portal.

Protocol: In Information Technology, a Protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols are often described in an industry or international standard.

Public-Private Key: A Public Key is a value provided by some designated authority as a key that, combined with a Private Key derived from the Public Key, can be used to effectively encrypt messages and Digital Signatures. A system for using Public Keys is called a Public Key Infrastructure.

Service: A Service is a software module deployed on network accessible platforms provided by the Service Provider. Its interface is described by a Service description. It exists to be invoked by or to interact with a Service requestor. It may also function as a requestor, using other Services in its implementation.

Service Availability: In Information Technology, Service Availability refers to a Service that is continuously operational for a desirably long length of time. Since a computer system or a network consists of many parts in which all parts and components usually need to be present in order for the whole to be operational, critical points for high Service Availability center around backup and fail-over processing and data storage and access.

Service Provider: A company that provides to its Trading Partner Electronic Information Exchange Services that would otherwise have to be located in their own company computers. The Service Provider is the owner of the Services offered.

Smart Card: A Smart Card is an Authentication device about the size of a credit card but with an embedded microchip and memory that can be loaded with data.

URL: A Uniform Resource Locator (URL) is the address of a file or resource accessible on the Internet. The type of resource depends on the Internet application Protocol. The URL contains the name of the Protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

User: The User is a person within the Party's organization using the Portal Services to the Agreement.

User Profile: A User Profile is a record of User-specific data that define the User's working environment. The record can include display settings, application settings, and network connections. What the User sees on his or her computer screen, as well as what files, applications and directories they have access to, is determined by how the Portal Administrator has set up the User's Profile.

VPN: A Virtual Private Network ("VPN") is a private information network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a secure communication Protocol and security procedures involving Cryptography to encrypt Information before sending it through the public network and decrypting it at the receiving end.

Appendix 2: TPA Module for XML Services

The objectives of this Appendix are: (a) To specify the business framework of the XML Transactions and Standards that the Parties to the Trading Partner Agreement (hereinafter the "Agreement") are intending to operate and use; (b) To identify the Parties and define the technical means for the transport, Encryption, Digital Certificate exchange of XML messages, and support procedures as well.

2.1. RosettaNet Business Specifications

The Parties may agree in writing, upon the adoption by RosettaNet of additional or updated Standards versions, to amend this Appendix to include such changes.

The Parties agree that any portion of the RosettaNet Standards which aims to determine contract formation, change, cancellation, or other legal rights or remedies does not form a part of this Agreement or any other agreement between the Parties. The Parties further agree that if any provision of the RosettaNet Standards is found inconsistent with this Agreement, this Agreement shall control.

According to the Parties' role specified below for a PIP^{TM} exchange, each Party may electronically transmit to or receive from the other Party: (a) any of the RosettaNet PIP Specifications listed below; (b) any additional Specification listed below to amend a PIP; and (c) such additional Specifications which the Parties by paper-based written agreement add to this Appendix.

Any attachment sent as part of a Business Signal shall be solely for the internal use of the transmitting Party and shall have no force or effect between the Parties except as eventually specified below with respect to any applicable PIP.

Where required in a PIP and as specified below, Digital Signatures shall be applied using a cryptographic Public-Private Key pair issued by the Certificate Authority identified below.

This Appendix is governed by the general legal provisions of the Trading Partner Agreement, Version _____, effective date _________________.

This Appendix, and the Trading Partner Agreement, may be considered as a part of another related agreement: ____ (*title of the related agreement*), effective date ________________

2.2. RosettaNet Technical Specifications

Parties to the Agreement	Company Name	Company Representative	Effective Date
Company A			
Service Provider A			
Company B			
Service Provider B			

PIPs or PIP scenario to the Agreement	
PIP #1	Title: e.g. 5C1 V01.00.00 Distribute Product list
PIP #2	Title:
PIP #3	Title:
PIP #4	Title:
PIP #5	Title:
PIP #6	Title:
PIP #7	Title:
PIP #8	Title:
PIP #9	Title:
PIP #10	Title:

Company A		
IDENTIFICATION	Company Address:	
	Contact Person for PIP Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider	Name: Address: Responsible: Tel.: Fax: Email:

Company B		
IDENTIFICATION	Company Address:	
	Contact Person for PIP Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider	Name: Address: Responsible: Tel.: Fax: Email:

Company A		
COMMUNICATION	Protocol:	Name: e.g. HTTP Version: e.g. 1.1
	Production URL(s):	https://………………….. Notes:
	Quality & Assurance URL(s):	https://………………….. Notes:
	Test URL(s):	https://………………….. Notes: e.g. URL will return a welcome page; URL will return a reference text with date/time stamp; etc.
	Production IP Address:	
	Q & A IP Address:	
	Test IP Address:	
	Host Computer / Server System	
	Security	Digital Signature Requirements: …………………………
	Other Requirements / Specifications:	………………………… e.g. At least two separate environments for development and producti on are required.
ENCRYPTION	B2B Software / Infrastructure, SSL Server	Name: e.g. webMethods Version: e.g. 3.6 Cipher strength: e.g. 128 bits
	SSL Encryption Algorithm	Name: e.g. RSA Key Length: e.g. 1024 bits
	Other Requirements / Specifications:	PIP-specific, 3rd Party-specific, etc: …………………………
CERTIFICATE	Standard / Policy	Name: e.g. X.509 Version: e.g. V1
	Expiration / Validity Period	Validity (start / end Date): …………………………
	Signature Algorithm	Name: e.g. RSA-MD5
	Exchange Method:	………………………… e.g. by encrypted email, by registered post,…
	Certificate Authority (CA)	Name: e.g. VeriSign Other CA Supported: ……………………
	File Format:	………………………… e.g. DER Format
	Other Requirements / Infrastructure Specs:	e.g. Sender must provide Certificate for Authentication

Company B		
COMMUNICATION	Protocol:	Name: Version:
	Production URL(s):	https://………………….. Notes:
	Quality & Assurance URL(s):	https://………………….. Notes:
	Test URL(s):	https://………………….. Notes:
	Production IP Address:	
	Q & A IP Address:	
	Test IP Address:	
	Host Computer / Server System	
	Security	Digital Signature Requirements:
	Other Requirements / Specifications:	
ENCRYPTION	B2B Software / Infrastructure, SSL Server	Name: Version: Cipher strength:
	SSL Encryption Algorithm	Name: Key Length:
	Other Requirements / Specifications:	PIP-specific, 3rd Party-specific, etc:
CERTIFICATE	Standard / Policy	Name: Version:
	Expiration / Validity Period	Validity (start / end Date):
	Signature Algorithm	Name:
	Exchange Method:	
	Certificate Authority (CA)	Name: Other CA Supported:

	File Format:	
	Other Requirements / Infrastructure Specs:	

ROSETTANET STANDARDS		
	Partner Interface Process PIP #1	Name: e.g. 5C1 Distribute Product List Version: e.g. V01.00 Notes: e.g. PIP Specifications' exchange is required for version verification; see Supporting Documentation.
	RosettaNet Implem. Framework (RNIF)	Name / Version: e.g. RNIF 1.1 Date: …………………………
	RosettaNet Technical Dictionary	Name / Version: e.g. RNTD 1.0 (or: not relevant for this PIP) Date: …………………………
	Global Transaction Code	e.g. Distribute Product List
	PIP Flow Direction	e.g. Initiator of PIP Transaction is Company B
	Supporting Documents, Values, Specifications, Business Rules	• e.g. Please refer to RNIF Technical Advisory A, 01.00.00, for PIP version • e.g. Empty XML optional element must not be transmitted in order to reduce file size and to avoid validation errors. • Please, for details see attached PIP Specification
	Company A	
	DUNS and DUNS+4 Number(s):	e.g. ST NV Swiss Branch: 488132309 ST USA: 065174484 ST Singapore: ……… ST Japan: ………
	Global Partner Role Classification Code:	e.g. Seller
	Global Partner Classification Code:	e.g. Manufacturer
	Global Supply Chain Code	e.g. Electronic Components
	Company B	
	DUNS and DUNS+4 Number(s):	
	Global Partner Role Classification Code:	e.g. Buyer
	Global Partner Classification Code:	e.g. Original Equipment Manufacturer
	Global Supply Chain Code	e.g. Electronic Components

OPERATION AND SUPPORT	**Company A**	
	Response Times for Confirmation Messages and Business Signals	Specifications (mandatory / agreed): e.g. Exceptions or further Specifications agreed by the Parties including variations of Confirmation requirements (Receipt / Acceptance)
	Failure Procedures	Specifications, if any:
	Service Availavility	Specifications, if any:
	Service Level Support	Specifications, if any:
	Other Requirements / Specifications:	Specifications, if any:
	Company B	
	Response Times for Confirmation Messages and Business Signals	Specifications (mandatory / agreed):
	Failure Procedures	Specifications, if any:
	Service Availavility	Specifications, if any:
	Service Level Support	Specifications, if any:
	Other Requirements / Specifications:	Specifications, if any:

2.3. Glossary

Business-to-Business: Business-to-Business (“B2B”) means business Transactions conducted over public networks, including Transactions that use the Internet as a delivery vehicle. Financial transfers, online exchanges, delivery of products and Services, supply chain activities, and integrated business networks are all examples of B2B.

Business Signal: A message exchanged between two RosettaNet network applications to communicate certain events within the execution of a PIP instance. Examples of Business Signals include Confirmation of Receipt and successful validation of a message. A Business Signal can be used to communicate an exception condition within the normal message choreography of a PIP.

Certificate Authority: A Certificate Authority (“CA”) is an authority in a network that issues and manages security credentials and Public Key for message Encryption. A CA associates Digital Certificates with a specific person or entity, identifies the person or entity that is to receive a Digital Certificate, issues and revokes these when required, and provides notice of revocations in a published Certificate revocation list.

Cipher: A Cipher is any method of encrypting text. It is also sometimes used to refer to the encrypted text message itself.

Cryptography: Cryptography is the science of Information security. Modern Cryptography concerns itself with the following four objectives: (a) Confidentiality (the Information cannot be understood by anyone for whom it was unintended); (b) Integrity (the Information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected); (c) Non-repudiation (the creator/sender of the Information cannot deny at a later stage his or her intentions in the creation or transmission of the Information); (d) Authentication (the sender and receiver can confirm each others identity and the origin/destination of the Information).

Digital Certificate: A Digital Certificate (in short: “Certificate”) is an electronic identification containing the credentials to operate business Transactions via Internet. A Certificate is issued by a CA and contains the owner’s name, a serial number, the expiration dates, a copy of the Certificate Public Key, which is used for Encryption and Digital Signature, and the Digital Signature of that Certificate Authority to allow a recipient for verification of Certificate validity.

Digital Signature: A Digital Signature is an Electronic Signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

DUNS ® Number: The Data Universal Numbering System (“DUNS”) is a sequentially generated nine-digit number that is assigned and maintained only by Dun and Bradstreet (D&B: http://www.dnb.com), which identifies unique business locations, and is global in scope.

DUNS ® + 4 Number: In addition to the DUNS number, there is a DUNS + 4 number, which can be used as a four-digit extension to the DUNS number to indicate specific locations within a campus environment of a company. As opposed to the DUNS number, which is centrally assigned and maintained by D&B, the DUNS + 4 is assigned and maintained by the owning organization.

Electronic Signature: An Electronic Signature means an electronic sound, code, symbol, or process, attached to or logically associated with a contract or other document and executed or adopted by a person with the intent to sign the document.

Encryption: Encryption is the conversion of data by means of mathematical algorithms into a form (secret code) that cannot be easily understood by unauthorized people.

Global Partner Classification Code: RosettaNet code identifying a Partner's function in the supply chain. Examples of possible values are the following: Broker, Carrier, Contract Manufacturer, Customs Broker, Distribution Centre, Distributor, End User, End User Government, Financier, Manufacturer, Original Equipment Manufacturer, Reseller, Retailer, Shopper, Warehouser.

Global Partner Role Classification Code: RosettaNet code identifying a Partner's role in the supply chain. Examples of possible values are the following: Anonymous Buyer, Buyer, Catalog Producer, Customer, Demand Creator, Financier, Product Distributor, Product Information User, Product Provider, Product Supplier, Return Provider, Return Receiver, Return Requester, Sales Facilitator, Seller, Supplier.

Global Supply Chain Code: The code identifying the supply chain for the Partner's function, e.g. Information Technology and Electronic Components.

Global Transaction Code: The code identifying the name of the business activity and the Transaction dialog in the PIP Specification document. Examples of possible values are the following: Distribute Purchase Order Status; Cancel Subscription; Change Subscription; Create Purchase Order; Change Purchase Order; Query Price and Availability; Query Product Information; Request Quote; Distribute Registration Status; Distribute Product List.

IP Address: The Internet Protocol (in short: “IP”) is the method or Protocol by which Information and data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP Address that uniquely identifies it from all other computers on the Internet. When Information is transmitted, the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address.

Key: In Cryptography, a Key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the Key (e.g 1028 bits) is a factor in considering how difficult it will be to decrypt the text in a given message.

PIP^{TM} (Partner Interface Process^{TM}): A Partner Interface Process ("PIP") is the RosettaNet^{TM} model based on XML documents containing Information and data that depicts the activities, decisions and Trading Partner role interactions that fulfil a B2B Transaction between two Trading Partners.

Protocol: In Information Technology, a Protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols are often described in an industry or international Standard.

Public-Private Key: A Public Key is a value provided by some designated authority as a key that, combined with a Private Key derived from the Public Key, can be used to effectively encrypt messages and Digital Signatures. A system for using Public Keys is called a Public Key Infrastructure.

RNIF: The RosettaNet Implementation Framework ("RNIF") provides implementation guidelines for those Trading Partners who wish to create interoperable software application components that execute PIPs.

RosettaNet: RosettaNet^{TM} is an independent, self-funded, non-profit consortium[6] dedicated to the development and deployment of Standard electronic business interfaces to align the processes between supply chain Trading Partners on a global basis.

Service: A Service is a software module deployed on network accessible platforms provided by the Service Provider. Its interface is described by a Service description. It exists to be invoked by or to interact with a Service requestor. It may also function as a requestor, using other Services in its implementation.

Service Availability: In Information Technology, Service Availability refers to a Service that is continuously operational for a desirably long length of time. Since a computer system or a network consists of many parts in which all parts and components usually need to be present in order for the whole to be operational, critical points for high Service Availability center around backup and fail-over processing and data storage and access.

Service Provider: A company that provides to its Trading Partner Electronic Information Exchange Services that would otherwise have to be located in their own company computers. The Service Provider is the owner of the Services offered.

Specification: The RosettaNet Specification is the complete documentation set of business and technical requirements and procedures that apply to the exchange of a PIP.

SSL: The Secure Sockets Layer ("SSL") is a commonly used Protocol for managing the security of a message transmission on the Internet. SSL uses the Public-Private Key Encryption system from RSA Security Inc., which also includes the use of a Digital Certificate.

Technical Dictionary: The RosettaNet Technical Dictionary provides common language for defining products and Services. In RosettaNet, the Technical Dictionary serves as a *bridge* from form, fit, and function Specification to a product number.

Transaction: A Transaction means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct: (a) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) Services, and (iii) any combination thereof; and (b) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

URL: A Uniform Resource Locator ("URL") is the address of a file or resource accessible on the Internet. The type of resource depends on the Internet application Protocol. The URL contains the name of the Protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

XML: The Extensible Markup Language ("XML") is a language that is concerned with creating, sharing and processing Information. Similarly to the language of today's Web pages (the Hypertext Markup Language), XML is concerned with display and transport of content.

[6] For the RosettaNet Bylaws and Intellectual Property Policy see the supporting documentation in the Web site www.rosettanet.org.

Appendix 3: TPA Module for Electronic Data Interchange (EDI) Services

The objectives of this Appendix are: (a) To specify the business framework of the EDI Transactions and Standards that the Parties to the Trading Partner Agreement (hereinafter the "Agreement") are intending to operate and use; (b) To identify the Parties and define the technical means and requirements for the transport, security, support and operation for the exchange of EDI messages and to describe security and support procedures as well.

3.1. EDI Business Specifications

Each Party may electronically transmit to or receive from the other Party: (a) any of the EDI Transaction Sets specified and according to the Standards listed below; (b) any additional Transaction Sets which the Parties by paper-based written agreement add to this Appendix.

The Parties agree that selected Standards include, as applicable, all data dictionaries, segment dictionaries and transmission controls referenced in those Standards, but include only the Transaction Sets listed below.

The Parties agree that any note or special instruction sent as part of a Transaction Set shall be solely for the internal use of the transmitting Party and shall have no force or effect between the Parties except as eventually specified below with respect to any applicable Specification or guideline.

The Parties agree to notify each other when there are unforeseen disruptions in normal process or when changes are about to occur that have the potential of disrupting the use of EDI for Electronic Information Exchanges.

This Appendix is governed by the general legal provisions of the Trading Partner Agreement, Version _____, effective date ________________.

This Appendix, and the Trading Partner Agreement, may be considered as a part of another related agreement: _______________________________________ (*title of the related agreement*), effective date _______________.

3.2. EDI Technical Specifications

Parties to the Agreement	Company Name	Company Representative	Effective Date
Company A			
Service Provider A			
Company B			
Service Provider B			

Company A		
IDENTIFICATION	Company Address:	
	Contact Person for EDI Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Technical Contact	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider (VAN)	Name: Address: Responsible: Tel.: Fax: Email:

Company B		
IDENTIFICATION	Company Address:	
	Contact Person for EDI Deployment	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Technical Contact	Name: Title: Address: Dept: Responsibility: Tel.: Fax: Email:
	Service Provider (VAN)	Name: Address: Responsible: Tel.: Fax: Email:

Company A		
COMMUNICATION (Point-to-Point)	Standard:	Name / Version: e.g. EDIINT AS1
	Protocol:	Name / Version: e.g. SMTP
	Production Address:	e.g. edi.prod@company.com Notes: …………………………
	Test Address:	e.g. edi.test@company.com Notes: …………………………
	Host Computer / Server System	e.g. HP, Unix
	Security Requirements	e.g. S/MIME required
	Other Requirements / Specifications:	e.g. Maximum message size:________

EDI ENVELOPE	Production envelope	UNB or ISA ID: e.g. STMPROD UNB or ISA QUALIFIER: e.g. ZZ
	Test envelope	UNB or ISA ID: ………………………… UNB or ISA Qualifier: …………………………
ENCRYPTION	B2B Software / Server Infrastructure	Name: e.g. Templar Version: 4.2
	Standard:	Name: e.g. S/MIME Version: V2 MPS
	File Encryption Algorithm (Symmetric Key)	Name: e.g. RC4 Key Length: e.g. 128 bit
	Other Requirements / Specifications:	EDI message-specific, 3rd Party-specific, etc: …………………………
CERTIFICATE	Standard / Policy	Name: e.g. X.509 Version: e.g. 3
	Expiration / Validity Period	Validity (start / end Date): …………………………
	Signature Algorithm	Name: e.g. RSA-SHA1 with S/MIME Key Length: e.g. 1024 bit
	Exchange Method:	e.g. by encrypted email
	Certificate Authority (CA)	Name: ………………………… Other CA Supported: ……………………
	File Format	e.g. CER format
	Other Requirements / Infrastructure Specs:	………………………… e.g. Sender must provide Certificate for initial Authentication
ACKNOWLEDGE-MENT	Message Disposition Notification	………………………… e.g. Acknowledgement required….

Company B		
COMMUNICATION (Point-to-Point)	Standard:	Name / Version:
	Protocol:	Name / Version:
	Production Address:	Notes:
	Test Address:	Notes:
	Host Computer / Server System	
	Security Requirements	

	Other Requirements / Specifications:	
EDI ENVELOPE	Production envelope	UNB or ISA ID: UNB or ISA QUALIFIER:
	Test envelope	UNB or ISA ID: UNB or ISA Qualifier:
ENCRYPTION	B2B Software / Server Infrastructure	Name: Version:
	Standard:	Name: Version:
	File Encryption Algorithm (Symmetric Key)	Name: Key Length:
	Other Requirements / Specifications:	EDI message-specific, 3rd Party-specific, etc:
CERTIFICATE	Standard / Policy	Name: Version:
	Expiration / Validity Period	Validity (start / end Date):
	Signature Algorithm	Name: Key Length:
	Exchange Method:	
	Certificate Authority (CA)	Name: Other CA Supported:
	File Format	
	Other Requirements / Infrastructure Specs:	
ACKNOWLEDGE-MENT	Message Disposition Notification	

EDI STANDARDS		
	Transaction Set #1	Standard: e.g. EDIFACT Organization: e.g. EDIFICE Reference: e.g. UN/EDIFACT DIRECTORY Document Name: e.g. ORDERS Description: e.g. PURCHASE ORDERS Version / Release: e.g. D.97A Revision: e.g. 7 Controlling Agency: e.g. UN Organization Specification ID: e.g. EDIPO04 Date: e.g. September 24, 1997 Recommendation: e.g. EDIFICE; Operation requirements according to _________ EDI Model.
	Supporting Documents, Values, Specifications, Business Rules	………………………
	Company A	
	Other EDI-related Standard Specifications	e.g. Please refer to the attached ORDER Guidelines.
	Company B	
	Other EDI-related Standard Specifications	………………………

OPERATION AND SUPPORT	**Company A**	
	Response Times for Confirmation Messages and Business Signals	Specifications (mandatory / agreed): e.g. Exceptions or further Specifications agreed by the Parties including variations of Confirmation requirements (Receipt / Acceptance)
	Failure Procedure	Specifications, if any: e.g. Alert after ___ minutes if no confirmation of receipt is transmitted. Action: e.g. email notification or file retransmission.
	Service Availavility	Specifications, if any:
	Service Level Support	Specifications, if any:
	Other Requirements / Specifications:	Specifications, if any:
	Company B	
	Response Times for Confirmation Messages and Business Signals	Specifications (mandatory / agreed):
	Failure Procedure	Specifications, if any:
	Service Availavility	Specifications, if any:
	Service Level Support	Specifications, if any:
	Other Requirements / Specifications:	Specifications, if any:

3.3. Glossary

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), Authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the User is authentic. The use of Digital Certificates issued and verified by a CA as part of a Public Key Infrastructure is considered likely to become the standard way to perform Authentication on the Internet

Business Signal: A message exchanged between two RosettaNet network applications to communicate certain events within the execution of an EDI message. Examples of Business Signals include confirmation of receipt and successful validation of a message. A Business Signal can be used to communicate an exception condition within the normal message choreography of an EDI message.

Certificate Authority: A Certificate Authority ("CA") is an authority in a network that issues and manages security credentials and Public Key for message Encryption. A CA associates Digital Certificates with a specific person or entity, identifies the person or entity that is to receive a Digital Certificate, issues and revokes these when required, and provides notice of revocations in a published certificate revocation list.

Cryptography: Cryptography is the science of Information security. Modern Cryptography concerns itself with the following four objectives: (a) Confidentiality (the Information cannot be understood by anyone for whom it was unintended); (b) Integrity (the Information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected); (c) Non-repudiation (the creator/sender of the Information cannot deny at a later stage his or her intentions in the creation or transmission of the Information); (d) Authentication (the sender and receiver can confirm each others identity and the origin/destination of the Information).

Digital Certificate: A Digital Certificate (in short: "Certificate") is an electronic identification containing the credentials to operate business Transactions via Internet. A Certificate is issued by a CA and contains the owner's name, a serial number, the expiration dates, a copy of the Certificate Public Key, which is used for Encryption and Digital Signature, and the Digital Signature of that Certificate Authority to allow a recipient for verification of Certificate validity.

Digital Signature: A Digital Signature is an Electronic Signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

Electronic Data Interchange (EDI): Electronic Data Interchange ("EDI") is a Standard format for exchanging business Information and data. The Standard is ANSI X12 and was developed by the Data Interchange Standards Association. ANSI X12 is either closely coordinated with or is being merged with an international Standard, EDIFACT.

An EDI message contains a string of *Data Elements*, each of which represents a singular fact, such as a price, product model number, and so forth, separated by delimiter. The entire string is called a *Data Segment*. One or more data segments framed by a header and trailer form a *Transaction Set*, which is the EDI message unit of transmission.

Electronic Signature: An Electronic Signature means an electronic sound, code, symbol, or process, attached to or logically associated with a contract or other document and executed or adopted by a person with the intent to sign the document.

Encryption: Encryption is the conversion of data by means of mathematical algorithms into a form (secret code) that cannot be easily understood by unauthorized people.

Key: In Cryptography, a Key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the Key (e.g 1028 bits) is a factor in considering how difficult it will be to decrypt the text in a given message.

Protocol: In Information Technology, a Protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols are often described in an industry or international Standard.

Public-Private Key: A Public Key is a value provided by some designated authority as a Key that, combined with a Private Key derived from the Public Key, can be used to effectively encrypt messages and Digital Signatures. A system for using Public Keys is called a Public Key Infrastructure.

Service: A Service is a software module deployed on network accessible platforms provided by the Service Provider. Its interface is described by a Service description. It exists to be invoked by or to interact with a Service requestor. It may also function as a requestor, using other Services in its implementation.

Service Availability: In Information Technology, Service Availability refers to a Service that is continuously operational for a desirably long length of time. Since a computer system or a network consists of many parts in which all parts and components usually need to be present in order for the whole to be operational, critical points for high Service Availability center around backup and fail-over processing and data storage and access.

Service Provider: A company that provides to its Trading Partner Electronic Information Exchange Services that would otherwise have to be located in their own company computers. The Service Provider is the owner of the Services offered.

Specification: The EDI Specification is the complete documentation set of business and technical requirements and procedures that apply to the exchange of an EDI message.

Transaction: A Transaction means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct: (a) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) Services, and (iii) any combination thereof; and (b) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.