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.