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.