

Overview

GDSN Security



Delivery Date: 08/01/07
Version Number 1.10
Disposition: **Final**

Document Summary

Version Number	1.10
File Name	GDSN_Security_v1 1-from2007Aug 20 SMH (4)
Delivery Date	08/01/07
Owner	GDSN Inc.
Description	GDSN Security Document

Document Revision History

Version Number	Date of Change	Changed By	Revision Description
1.0	05/21/2007	Sean Lockhead	Moved to V1.0 Final
1.1	08/01/2007	Sean Lockhead	Resolve comments from Legal Review

Disclaimer

Whilst every effort has been made to ensure that the guidelines to use the GS1, GDSN, Inc. standards contained in the document are correct, GS1, GDSN, Inc. and any other party involved in the creation of the document HEREBY STATE that the document is provided without warranty, either expressed or implied, of accuracy or fitness for purpose, AND HEREBY DISCLAIM any liability, direct or indirect, for damages or loss relating to the use of the document. The document may be modified, subject to developments in technology, changes to the standards, or new legal requirements. Several products and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Table of Contents

1 EXECUTIVE SUMMARY	5
1.1 Introduction	5
1.2 Choreography	6
2 PRE-EXISTING COMMUNICATIONS PLATFORMS	8
2.1 Traditional EDI Security	8
3 COMMON ELEMENTS	10
3.1 GDSN Data	10
3.2 Transport Protocols	10
3.2.1 Encryption	10
3.2.2 Digital Certificates	10
3.3 GDSN Data Ownership	11
3.4 GDSN Security Certification Considerations	11
4 GDSN REGISTRY	12
4.1 Summary – Global Registry	12
4.2 Physical	12
4.2.1 Database	12
4.3 Compliance	13
4.4 Legal	13
4.4.1 Service Level Agreements (SLA)	13
4.5 Communication within the GDSN	13
4.5.1 Data Communication	13
4.6 Trading Partner Security Concerns	13
4.7 GDSN Global Registry Security Certification Considerations	14
5 TRADING PARTNER TO SOURCE DATA POOL	15
5.1 Summary	15
5.2 Synchronisation Process Flow	15
5.3 Communication of Synchronisation Data	15
5.3.1 Data Communication	15
5.3.2 Transport Protocols	16
5.3.3 Data Pool Value-Added Services	16
6 SECURITY AT SOURCE DATA POOL	17
6.1 Summary	17
6.2 Mutual Legal Agreements	17
6.3 Data Stored vs. Data Passed	17
6.4 Data Access	17

6.5	SDP Security Concerns.....	18
6.5.1	Principles Restated (Pricing)	18
6.6	Conclusion	18
7	SECURITY FROM SDP TO RDP	19
7.1	Summary	19
7.2	Legal Agreements	19
7.3	Compliance to Standards	19
7.4	Valid XML Message Creation	19
7.5	GDSN Certification	19
7.6	SDP to RDP Security Concerns	19
7.6.1	Priority / Applicability of Multiple Agreements	19
8	SECURITY AT RECIPIENT DATA POOL	21
8.1	Recipient Data Pool Role	21
8.2	Recipient Data Pool Role Options.....	21
8.2.1	Pass Through Implementation of RDP Services.....	21
8.2.2	Repository Services.....	21
8.3	Redundant GDSN Validations	22
8.4	General Security.....	22
8.4.1	Data Pool Messaging	22
9	SECURITY FROM RECIPIENT DATA POOL TO DATA RECIPIENT23	
9.1	Summary	23
9.2	Message Process Flow	23
9.3	Message Validation	23
9.4	Synchronisation List	23
9.5	Communication of GDSN Data.....	23
9.6	Communication of Synchronisation Data	24
9.6.1	Data Communication	24
9.6.2	Transport Protocols	24
9.6.3	Data Pool Value-Added Services	24
9.6.4	Data Pool Value Added Services	25
9.7	Authorisation.....	25
9.8	Access Control	25
10	THIRD PARTY AUDITS	26
10.1.1	Summary	26
10.1.2	Trading Partner Agreements	26
10.1.3	Third Party Audit Discussion Guide.....	26
A.	IMPLEMENTATION CONSIDERATIONS	27
A.1	Security.....	27
A.2	Anti Virus	27

A.3	Password & PIN Security	28
A.4	Network & Computing Resources	28
A.5	Backups & Disaster Recovery	28
B.	COMMENTS FROM GS1 AUSTRALIA	30
C.	SAS 70	31
C.1	SAS 70 Overview	31
C.2	Service Auditor's Reports	31
C.3	Benefits to the Service Organization	32
C.4	Benefits to the User Organization	33
D.	ISO 17799	34
D.1	Overview.....	34
D.2	The Contents of the Standard	34
D.3	Certification and Compliance.....	35
E.	SAMPLE EXISTING TRADING PARTNER TO TRADING AGREEMENT	37

1 Executive Summary

1.1 Introduction

In order for the strong commitment to the vision and principles of Global Data Synchronisation, to be achieved, standard, compliant product information must be able to flow uninterrupted between trading partners in a secure fashion. The exchange of supply chain information carries the greatest risk when not handled securely, but carries the greatest rewards when handled securely.

One of the key considerations for ensuring the usability and wide adoption of the GDSN Network is the security needs and concerns involved in implementing and interacting with such a network. Responding to concerns expressed both from the community and the industry at large, GDSN has collaborated on this proposed strategy for developing a set of security guidelines that address all aspects of security (physical, logical, business processes and contractual).

This security document is intended to fully define the breadth and depth of the aspects and various components of security for GDSN. It describes the GDSN proposed strategy for addressing security of data within the GDSN network, as well as beyond the network, to include recommendations for the relationship between source / recipient data pools and suppliers / retailers.

Security is addressed in all related aspects with the goal of ensuring confidence in the retailer / supplier that the storage and handling of their data is secure at all times throughout the process both in / out of GDSN network. As such, security must be addressed at several levels within and throughout the process, which includes participants beyond the Global Registry, beginning with the Data Source (Supplier), to the Source Data Pool, to the Recipient Data Pool, and finally the Data recipient (retailer). The insurance of GDSN security depends on the point in the process, different solutions, measures and / or controls.

Key Principles regarding GDSN and the security of data within and beyond the network are:

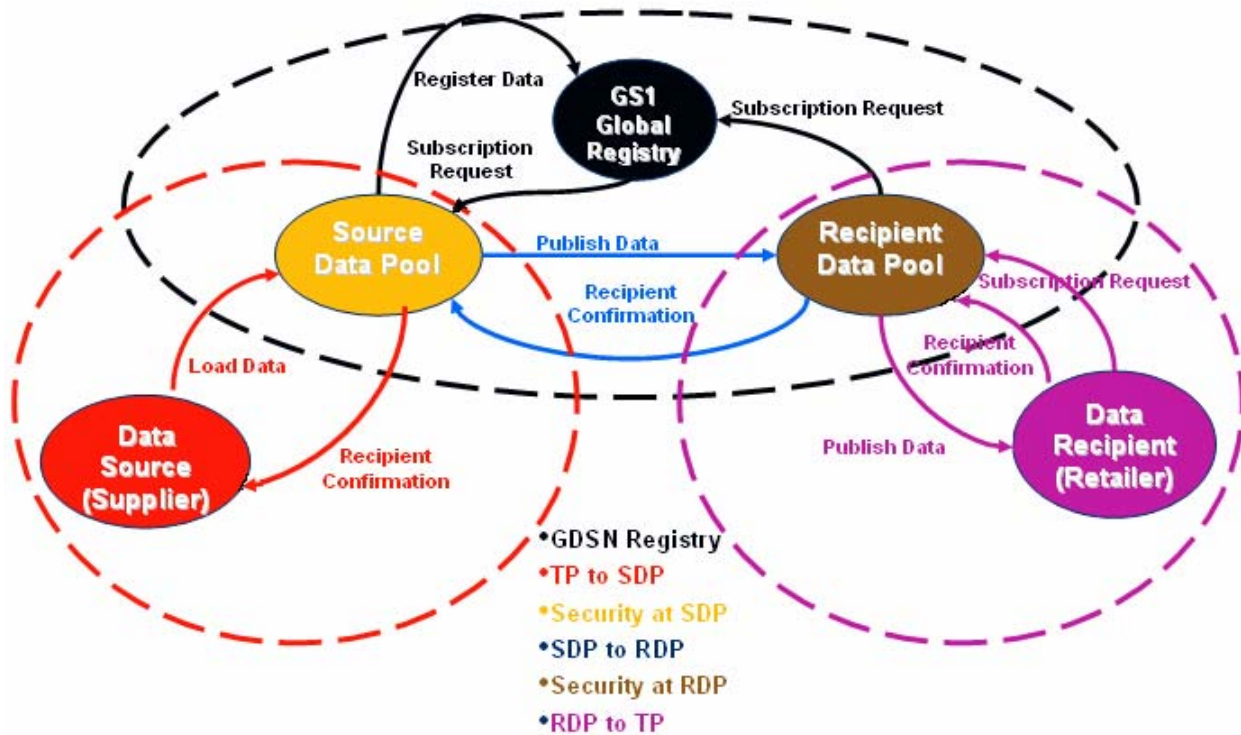
- GDSN is an enabler and can provide guidance / insight to Data Pools and Trading Partners to ensure a comfort level with Trading Partner relationships, but ultimately, it is the Trading Partner to Trading Partner agreements that should reflect / guide security expectations around how data is handled and this then guides DP (TP/DP). (DP/DP) agreements.
- It is recognized that some levels of security is not required for all types of data
- GDSN Certification requires certain levels of security (AS2)

The sections in this document correspond to the GDSN Choreography (defined below), showing the end-to-end flow of data, the GDSN network and where the lines of authority are regarding mandatory and recommended security requirements.

The information contained in this document represents the current view of GDSN, Inc. and may change over time with the evolution of technology, security best practices, and supply chain automation.

1.2 Choreography

GDSN CHOREOGRAPHY



RELATIONSHIP SCENARIOS:

Information Technology Platform Ownership

Companies have an almost limitless variety of options of how to manage their information technology (IT) infrastructure. In the simplest scenario a Company owns all IT assets, runs them in a facility they own, manages the infrastructure themselves and they manage and administer the applications.

While this is not a comprehensive list, some commonly used IT infrastructure management options include:

- Leased IT assets (processors, hard drives, network equipment, communication lines, etc) from a financing company
- Leased IT assets and have them running in a shared data center
- Own IT assets and have them running in a third party data center

- Leased network services between facilities owned by the company
- Outsource to a third party the operation of data center and all IT assets
- Outsource the running of a business application to a third party
- Outsource all IT infrastructure operations
- Use a hosted application run by a third party
- Use part of a shared service run by a third party

Additionally, with the advent of telecommuting, Wi-Fi hotspots, Virtual Private Networks (VPN), use of personally owned computers, etc, many of the above scenarios get even more complex.

Frequently, the ownership of IT assets is difficult to discern, even to members of the IT department. Due to the constant reallocation of scarce resources, many large companies are a combination of all of the above models with numerous variations.

2 Pre-Existing Communications Platforms

There is a lot of electronic commerce (peer to peer, hard copy, phone / fax, manual transfer of data via disk or CD, etc) that transpires today, of which EDI is the one most commonly accepted.

In an attempt to more fully understand how existing systems influence the ongoing GDSN requirements, it is important to understand what is in place today and how it influences trading partner security implementations and issues.

2.1 Traditional EDI Security

- There are an enormous amount of business transactions being sent using EDI today. Common examples of these are
 - Prices
 - Item catalogues
 - Orders
 - Invoices
 - Payment advices
- EDI transactions frequently transfer through multiple EDI Value Added Networks (VAN's). The relationship between VAN's is covered under EDI interconnect agreements. However, there are no mentions of security requirements in the context of the underlying data in the typical interconnect agreements. From a typical VAN interconnect agreement, "The relationship between the parties shall be that of independent contractors." There is rarely a contract between the trading partners on one VAN and the interconnected VAN.
 - Currently, contracts (referred to as interconnect agreements) between VAN's do not specify security aspects or data ownership stipulations.
- Transfer of data between VAN's is typically through frame relay or leased line connections. Protocols typically in use are FTP, Bisynchronous and X.435.
- EDI VAN's traditionally run highly secure data centers and highly secure operations. Access to the underlying data contained in EDI transactions are controlled by security policies and procedures implemented by each EDI VAN. The policies and procedures are proprietary to each company and are not published for reasons of competitiveness and to not expose the security. These processes typically include:
 - Limiting the physical access to the machines containing data
 - Limiting access to these systems through firewalls, password protection, and personal user accounts to manage access control.
 - Allowing individuals to access only the data that is required for them to perform their jobs.

- There are other third party solutions within the supply chain, for example Service Bureaus. These third party relationship(s) exist in many contexts and play a key role in the supply chain. The definition of and dissemination of this information provides for additional potential information to be introduced into the supply chain. In addition, the complexity also increases as does the chance for establishing multiple points of reference for the same data. These services have existed and will continue to exist to support an existing business need.
 - Open Define Service Bureau (incorporate definition)

Web based portals exist that are trading partner specific. Security may vary and may be inconsistent across different portals. The relationship of the trading partners would dictate the expectations of security.

3 Common Elements

3.1 GDSN Data

GDSN Data can be viewed as Party, Trade Item, Catalogue Item, Price, or any other information that is communicated in the Global Data Synchronisation Network. The processes for the dissemination of this information are related and are based on similar messaging. An effort is made to try and address both the similarities as well as the differences.

3.2 Transport Protocols

In the GDSN, the only transport protocol is the use of electronic data over the public Internet, Applicability Statement 2 (EDIINT AS2). This is a mandatory requirement for Data Pools and the Global Registry in the GDSN. For additional information, please refer to the EDIINT AS2 implementation document and the latest version of the GDSN Operations Manual.

The AS2 protocol uses the Hyper Text Transmission Protocol (HTTP). The AS2 specification solely describes the secure transmittal of data over the Internet using HTTP. It is a specification on securing and transporting data, not on validating or processing the data. The transported data is then dispatched to the appropriate processor based upon its content-type.

3.2.1 Encryption

Encryption is a critical part of secure data handling. Data messages communicated between all parties in the GDSN network, including Data Pools and the GS1 Global Registry, are encrypted by the use of EDIINT AS2 protocol. Beyond GDSN there can be other types. There are different levels of encryption:

- Transport Protocol Message encryption (EDIINT AS2)
- Data (Payload) Encryption
 - Full – Encryption of entire payload – Requires additional content.
 - Partial – Encryption of certain individual attributes value(s) within the payload.
Note: Attribute values encryption is above and beyond the current scope of the GDSN and would only be recommended if the function is needed.

There are no standards governing the storage of data in the Data Pools nor the communication processes between the data pools and their trading partners. Internal storage and encryption of the data is based on the business relationship between the Data Pool and its trading partners. For example, price synchronisation security obligations may be managed by the mutual agreement of the data pool and its members.

3.2.2 Digital Certificates

Certified Data Pools must use a self-signed digital certificate or a signed digital certificate from a recognized third party organization that is responsible for the issuance of these types of digital certificates. All Data Pools and the Global Registry must implement the use of digital certificates and maintain an up-to-date listing of all the other Data Pools and Global Registry digital certificates.

Any use of a digital certificate between a data pool and their trading partners would be handled within their relationship agreement. Refer to the operations manual in regards to any additional digital certificate information or EDIINT AS2 information.

3.3 GDSN Data Ownership

Data Pool security issues and concerns to be addressed and resolved include primarily the establishment of the chain of custody and ownership of the data as it moves through the supply chain. The “ownership” of the data dictates what operations may be performed and by whom at each point in the chain. Based on the previous statement it may be assumed that the retailer owns the rights to distribute the data they received from the supplier. This aspect of the relationship is typically governed by the terms of a trading partner agreement. There are typically provisions for either trading partner to store the data in any form they prefer, provided it is satisfactory to mutual agreements with trading partners.

The following considerations should be taken in account:

- The contractual agreements between the trading partners and their data pools and govern the data ownership, confidentiality, and responsibilities of the maintenance and distribution of GDSN Data. There may also be trading partner to trading partner agreements without Data Pools in the context of trading partner data.
- When the Data Source initiates publication of their data to a trading partner, the data to be communicated is going to be sent to the correct Data Recipient.
- At the time the data is published to the trading partner, the data is exposed to the Data Recipient.
- The Data Source and the Data Recipient are responsible for controlling what actions may be taken with this data and protecting the confidentiality of the data.
- There are third party agreements that may be in place to protect the confidentiality.

It is highly recommended that there are trading partner to trading partner agreements in place to handle all general concerns and issues.

Today trading partner agreements governing data confidentiality and usage may not exist, may not be legally binding, or may be too vague to be of value. The establishment of this level of detail is left up to individual Trading Partners.

GDSN Inc. strongly recommends and encourages Trading Partners to have confidentiality agreements in place (from business and technical perspective) with all business partners and to include the detailed requirements in the agreements.

Appendix E references a typical Trading Partner agreement that may be in place today.

3.4 GDSN Security Certification Considerations

The GDSN certification process should ensure that data pools and the GS1 Global Registry, at a minimum, demonstrate the following:

- Successful completion of a third party administered security audit (when defined)
- AS2 compliant transport and compliance with applicable AS2 operational requirements
- Compliance with the GDSN synchronisation BUSINESS MESSAGE STANDARD (BMS), data attribute, messaging and processing requirements
- Adequate access controls are in place to ensure data is exposed only to the appropriate data recipients

4 GDSN Registry

4.1 Summary – Global Registry

The Global Registry is responsible for ensuring that trading partners registered at the Global Registry (members of GDSN) pass the GDSN-mandated validations. Through the use of the basic party synchronisation process, the Global Registry communicates all validated Trading Partners (GLN's) to all Data Pools for use in the GDSN Business Message Standard use cases, i.e. all the GDSN-specific processes.

The Global Registry is responsible for ensuring that registry catalogue items (“Items”) registered at the Global Registry have passed the GDSN-mandated validations and have been registered by previously registered, validated Parties (GLN) already present in the Global Registry. Through the use of the Catalogue Item Synchronisation process, the Global Registry enables the Data Pools to communicate the standards-based business message standard messages for all the use cases.

The Global Registry is responsible for ensuring that catalogue items subscriptions (“Subscriptions”) registered at the Global Registry have passed the GDSN-mandated validations and have been registered by registered, validated Parties (GLN). The Global Registry Item / Subscription matching process functionally provides the Data Pools and Trading Partners the information necessary to perform the GDSN use cases. The Global Registry distributes subscriptions to one or more Data Pools having registered items that can fulfill the subscription criteria. Through the use of the Catalogue Item Synchronisation process, the Global Registry enables the Data pools to communicate the standards-based business message standard messages for all the use cases.

4.2 Physical

4.2.1 Database

Access to the Global Registry is restricted to authorized personnel of the GS1 US Technology Services Group (TSG) as the technology service provider of the Global Registry for GDSN Inc.

The GDSN Customer Support has access to the information contained in the Global Registry, as well as messaging to and from the Global Registry.

Data access types for Global Registry personnel are as follows:

- Add – who / what can add, how is managed / restricted
- Change – who / what can add, how is managed / restricted
- Delete – who / what can add, how is managed / restricted

The GDSN Customer Service is the communication point for handling all requests for data audits and message delivery verifications.

The GDSN Customer Service can track and detail the requester, the resolution, and the specifics of the resolution/response.

4.3 Compliance

The Global Registry must successfully complete all certification events and remain compliant with the GDSN Certification Criteria Document for participation in the GDSN.

4.4 Legal

The Global Registry is required to meet or exceed the Service Levels set forth in the GDSN Inc. Service Level Agreements. (For any additional information refer to Service Level Agreements).

4.4.1 Service Level Agreements (SLA)

- In terms of Security, it is the responsibility of the Global Registry to maintain a reference list of Certified Data Pools that can effectively communicate with the Global Registry. Each Data Pool has a set of information associated with it that is stored in the Global Registry.
- The function of setting up the Data Pools in the Global Registry is the responsibility of the GDSN Support Staff, operating under the direction of GDSN Inc. representatives and in unison with the GS1 Global Registry Service Provider.
- The Global Registry is required to process valid messages sent to it. It is agreed that scheduled outages, which have been communicated by the Global Registry to all affected Data Pools in the manner specified in this document, can affect the timeliness of the processing (e.g. processing can take place after the scheduled outage period).

4.5 Communication within the GDSN

The trading relationship between the Global Registry and the Data Pools covers how the data is communicated between the network entities.

For additional information, refer to GRALA (Global Registry Access and License Agreement).

4.5.1 Data Communication

All GDSN data is communicated using GS1 GDSN standards-based XML message(s).

4.6 Trading Partner Security Concerns

Concerns have been raised by the GDSN Trading Partners about information registered in the Global Registry. This is a cursory list that lists the main community concerns.

- Trading Partners are satisfied that any information registered in the Global Registry (parties, items, subscriptions) is only accessible by the authorized entities.
- Data pools and Trading Partners want to ensure that information communicated to and from the Global Registry to each entity is secured from an access-control, as well as an authorization perspective.
- As new functionality is added to the GR, additional requirements may surface.

4.7 GDSN Global Registry Security Certification Considerations

The GDSN certification process should ensure that Global Registry, at a minimum, demonstrates the following:

- Successful completion of a third party administered security audit (when defined)

5 Trading Partner to Source Data Pool

5.1 Summary

Source Data Pools have the ultimate responsibility for the communication of GDSN Data into the Global Data Synchronisation Network (GDSN). They are responsible for gathering the GDSN Data from their supply side trading partners, performing validations upon the data, registering the items in the Global Registry, managing that the data is sent to the correct trading partner or their GDSN-certified RDP and ensuring the data is compliant when distributed into the network. In the data synchronisation process, the role of the Source Data Pool is to perform the required standards-based actions on the Data. There are some remaining issues and concerns related to the Source Data Pools and their relationships with their trading partners.

5.2 Synchronisation Process Flow

The following steps represent the Source Data Pool responsibility as it relates to the GDSN Data synchronisation processing:

- The Source Data Pool receives GDSN Data from the Data Source.
- The Source Data Pool prepares the GDSN data for registration in the Global Registry.
- The Source Data Pool performs the required GDSN data validations, and, informs the Data Source of any errors encountered.
- The Source Data Pool interrogates a Synchronisation List that maintains the status of specified GDSN Data information sent to each Data Recipient, and uses this list to manage the distribution of ongoing GDSN Data.
- The Source Data Pool sends the Synchronisation document directly to the Data Recipient or their Recipient Data Pool.
- The Source Data Pool receives the Synchronisation Confirmation from the Data Recipient's Data Pool.
- The Source Data Pool updates the appropriate information in the Synchronisation List.
- The Source Data Pool forwards the Synchronisation Confirmation to the Data Source.

5.3 Communication of Synchronisation Data

The trading relationship between the Source Data Pools and their trading partners governs the requirements Source Data Pools have for how they receive data from their members, as well as additional value-added services they perform for those members. The relationship contracts detail how the data is received from the trading partner and what transport protocol is utilized. These services include additional data validations, transformation of the data in different formats, use of the data within other applications offered by the Source Data Pool.

5.3.1 Data Communication

Some examples of data communications used are:

- GDSN standards-based XML message
- Proprietary XML message
- User Interface
- Flat File
- EDI

GDSN Security Version: 1.10	Overview	Delivered on: 08/01/07
---------------------------------------	-----------------	----------------------------------

- Spreadsheet Applications
- Adobe® PDF
- Other

5.3.2 Transport Protocols

This communication path is not defined by GS1 and GDSN standards and therefore, out-of-GDSN communication. Some examples of transport protocols used are:

- EDIINT AS2
- Virtual Private Network (VPN)
- File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP)
- Electronic Data Interchange (EDI)
- E-mail
- Other

5.3.3 Data Pool Value-Added Services

Restrictions placed upon Source Data Pools that limit how they can handle GDSN Data information sent from trading partners could severely hamper the Source Data Pool's ability to perform or provide these services for their members. It may also limit the Source Data Pool's ability to comply with all of the GDSN Data synchronisation process requirements relating to validations, synchronisation list processing and maintenance. This potentially disrupts the ability to support the existing business process of their trading partners.

- GDSN Data applications
- Robust user interface allowing the Data Source to enter information directly into the Source Data Pool
- Workflow processing
- Supplier and/or Retailer specific validations
- Message and file level track and trace for audit or problem resolution
- Reporting
- Retransmission capabilities
- Other

6 Security at Source Data Pool

6.1 Summary

This document describes the proposed strategy for addressing security of GDSN Data at Source Data Pool within the GDSN network. A data source is normally synonymous with a manufacturer, however; may include other roles, e.g. distributor, broker, wholesaler, etc. There are different concerns of security that need to be addressed. Some of these concerns are real and some are perceived and not based in facts. Both need to be addressed.

6.2 Mutual Legal Agreements

Data Sources (suppliers, manufacturers, distributors, etc.) typically have a legal agreement with their solution provider that hosts their GDSN Data. The solution could be in the form of product catalogue, exchange, hosted web portal, EDI solution provider, etc. Because this security document is limited to the GDSN environment, only "Source Data Pool" requirements will be described.

GDSN network requirements for specific processing / handling of GDSN Data and additional constraints may limit the Data Pool's ability to deliver value-added services. The Source Data Pool must currently support all security requirements of their community.

6.3 Data Stored vs. Data Passed

There may be trading partner requirements that data not reside on the data pool but is passed to recipient for their own use. GDSN data that is not intended to be available to the community of the data pool (for viewing or download) and only "to be passed" is still stored there for the very short time until it is passed. If a trading partner has specific requirements for storage in the context of their relationship with their data pool, it is up to that specific trading partner to reach the agreement with the individual data pool that best meets those requirements.

6.4 Data Access

The community makes GDSN data available in many ways. Some GDSN data accesses are as follows:

- sent via message
- downloaded
- sent via EDI
- Viewed online

6.5 SDP Security Concerns

6.5.1 Principles Restated (Pricing)

These are basic principles of GDSN Data synchronisation that may need to be clearly restated for price synchronisation:

- In the GDSN context, the Data Source may not have a legal agreement with the RDP (unless they are on the same data pool). The Data Source should have an agreement with any Data Recipients, which has implications on how the data is handled and confidentiality maintained.
- A Data Source has a legal agreement with SDP, controlling the handling of the data and the confidentiality requirements.
- The SDP provides access to GDSN data only to the intended Data Recipient (if member of the same data pool)
- The SDP sends a secure encrypted message to the RDP of the Data Recipient

6.6 Conclusion

To establish a high confidence level for the exchange of GDSN data in the GDSN, there are recommended security guidelines for all participants. Some data (such as price-based data) have additional security requirements.

It is possible to add a security segment into the legal GDSN data pool agreement stating that the data pool agrees to make the data available only to the designated party. If the data recipient is a member of another data pool then only that data pool would get the data (i.e. a SDP can only guarantee that the data has been delivered to a RDP).

7 Security from SDP to RDP

7.1 Summary

As part of the GDSN, one of the most important stages of the synchronisation choreography is when information (item, party, price, etc.) is sent from the source side through the Network to the recipient side. It is at this point in the data synchronisation process information is exchanged in a way that is governed by standard messages and processes. All of the certified data pools are working in a standards-based, validated fashion.

7.2 Legal Agreements

At this level of communication in the GDSN, the binding agreements are facilitated by GDSN Inc. Although it is possible to have individual legal agreements between data pools that define certain functionalities and / or capabilities, the agreements are specific to that relationship. The GDSN Inc. agreements govern these particular relationships. A major point is that the agreement that the methods and functions of this exchange are governed consistently the same way for all certified GDSN Data Pools.

7.3 Compliance to Standards

The use of GS1 Standards and most specifically GDSN standards as outlined earlier in this section are mandatory for all in-network traffic. These standards allow for efficient adoption of the GDSN Data synchronisation processes.

7.4 Valid XML Message Creation

The Communication between the SDP and RDP occurs through standard, valid XML messages. The use of XML instance documents based on standardised XML schemas, as defined by GS1 Standards, is fundamental in the GDSN. Data Pools are free to engage in other value-add activities, but it is beyond the GDSN governance and cannot be enforced by the GDSN.

7.5 GDSN Certification

All Data pools operating in the Production GDSN environment where all the live synchronisation processes occur must have passed the GDSN certification process as defined by GDSN Inc. and GS1. There are limited certification criteria that impact the overall security of the GDSN, as most of the certification concentrates on the functionality.

7.6 SDP to RDP Security Concerns

7.6.1 Priority / Applicability of Multiple Agreements

1. DP – DP in GDSN

2. DP – DP non-GDSN
3. TP – DP
4. TP – TP

When there is more than one agreement in place, the following must occur:

- Ensure that there are no conflicts between the multiple agreements in place
- Establish which ones take precedence over the other(s)

8 Security at Recipient Data Pool

8.1 Recipient Data Pool Role

The role of the Recipient Data Pool (RDP) in the Global Data Synchronisation Network (GDSN) is to provide an interface between the GDSN and the data recipient. A data recipient is normally synonymous with a retailer, however; may include other roles, e.g. distributor, broker, wholesaler, etc. To perform the recipient role, the RDP receives GDSN standard messages from source data pools and the Global Registry, and routes the messages only to the recipient designated in the messages, possibly including third parties outside the GDSN.

8.2 Recipient Data Pool Role Options

The relationship between a RDP and the Data Recipient is not governed by the GDSN but by the company providing the RDP services. There are an almost unlimited number of implementation methodologies and details. The following sections describe some of those variations as background information for the further understanding of the security topics surrounding RDPs.

8.2.1 Pass Through Implementation of RDP Services

The RDP may implement as a pass through service. In this implementation, the RDP is used as a routing mechanism for messages that it receives through the GDSN. The RDP receives the GDSN messages and, based on parameters in the GDSN message, the RDP message is routed and delivered to the correct Data Recipient. In this case, the RDP may or may not store the data in the message, or portions of the message needed to perform other processes. However the RDP must examine the contents of the message to determine where the message should be going or where it originated. Many pass through applications must store a copy of the message. The possible uses for a copy of the message are audit, recovery of the message, or the retransmission of the message if there is a problem down stream from the pass through/routing application.

8.2.2 Repository Services

The RDP may act as a data repository on behalf of the data recipient. In this scenario, the RDP (and SDP) will hold the data for the recipient. This scenario has the data recipient responsible for security of supplier data based on its relationship with the recipient data pool. This type of solution is very common among data pools and solution providers. It allows for a staging arena for the recipient's data and for reloads of the data should a failure happen in the recipient's internal data repository. This should be based on a mutually-agreeable timeframe and not exceed the agreements between the Data Source and the Data Recipient and the Trading Partner and its Data Pool. In this scenario, the GDSN Data security is covered by several relationships.

The first relationship is a trading partner relationship. This is an agreement between two trading partners that governs the use and confidentiality of the data in the relationship. A trading partner agreement describes the use of data, by whom, for what and the penalties for breaches in the contracted use of data.

The second relationship is between the recipient Trading Partner and its data services provider. In this relationship the Recipient holds its data providers to an equal or higher level of security than is mandated by the Trading Partner agreement. There can be multiple service providers between the Data Source and Data Recipient, which are all responsible for upholding / maintaining integrity and security of the data. Such service providers include but are not limited to GDSN Recipient Data Pools' applications and application architecture, data bases and database architecture, service oriented architecture, data centers, long and short haul disaster recovery, on and off-site backup and recovery, third party solution partners, data transport mechanisms and protocols. There are limited specific requirements in terms of technology platform considerations.

8.3 Redundant GDSN Validations

Most implementations of Recipient Data Pools submit received messages through a validation check to ensure that the Source Data Pool that sends the message caught any data or formatting errors before sending the message. This is not mandatory but is the choice of the RDP to ensure that their customer (the data recipient) is receiving valid data.

8.4 General Security

8.4.1 Data Pool Messaging

The Recipient Data Pool can use any transmission protocol or method between the Recipient Data Pool and the Data Recipient.

The security for a messaging system relates to a chain of custody for that message and its GDSN Data. Each entity that holds or passes the GDSN Data needs to provide a record of the data while it was in their possession for two reasons. First, It is necessary to have the audit capabilities if there was a problem while the data moves from Data Source to Data Recipient so that there can be effective issue resolution. Second, if an error happens while attempting to transmit the GDSN data, the message persists for at least for a short period of time to allow for retransmission of the message. Since the method of transport between data pool and trading partner is not governed by the GDSN and there is no way to mandate this security measure.

9 Security from Recipient Data Pool to Data Recipient

9.1 Summary

Message Information at Recipient Data Pool involves a unique situation since the GDSN data at this stage of the choreography represents information received from elsewhere in the network.

9.2 Message Process Flow

The following steps represent the Recipient Data Pool responsibility as it relates to the GDSN Data synchronisation processing:

- The GDSN Data is received from the SDP.
- The RDP may perform GDSN data validations, and any additional validations. (note: there is no requirement that an RDP repeat the SDP validations)
- The RDP may implement a Recipient Synchronisation List that maintains the status of specified GDSN Data information sent to each Data Recipient, and is used to manage the distribution of ongoing GDSN Data.
- The RDP sends the GDSN Data directly to the Data Recipient.
- The Data Recipient receives the GDSN Data and makes a decision on whether or not to synchronise the GDSN Data.
- The RDP receives the Synchronisation Confirmation from the data recipient
- The RDP may update the appropriate information in the Synchronisation List.
- The RDP forwards the Synchronisation Confirmation to the SDP.

9.3 Message Validation

Any Validations that are defined by GDSN to be in-network validations, in which the RDP is the actor, must be run at the RDP. In addition, extra value-added validations may be run at the RDP. The RDP can communicate that information to the Data Recipient. However, it is imperative that the RDP cannot fail a message if all of the GDSN validations are passed.

9.4 Synchronisation List

An RDP may choose to maintain an optional Functional synchronisation list for use within the RDP. The synchronisation list of record is held at the Source Data Pool.

9.5 Communication of GDSN Data

The dissemination of GDSN Data by a Recipient Data Pool to Data Recipients requires that only the Data Recipients intended to receive the information (as determined by the message) are the entities that actually receive the messages, in whatever form, from the RDP.

9.6 Communication of Synchronisation Data

The trading relationship between the Recipient Data Pools and their trading partners governs the requirements Recipient Data Pools have for how they receive and transmit data for their members, as well as additional value-added services they perform for those members. The standards and implementation guides govern how the data is received from the trading partners and what transport protocol is utilized. These services could include additional data validations, transformation of the data from different formats, use of the data within other applications offered by the Recipient Data Pool and any other value-added services offered or performed by the Recipient Data Pool.

9.6.1 Data Communication

Some examples of data communications used are:

- GDSN standards-based XML message
- Proprietary XML message
- User Interface
- Flat File
- EDI
- Spreadsheet Applications
- Adobe® PDF
- Other

9.6.2 Transport Protocols

Since this is considered out of network communication, some examples of transport protocols used are:

- EDIINT AS2
- Virtual Private Network (VPN)
- File Transport Protocol (FTP), Secure File Transport Protocol
- Electronic Data Interchange
- E-mail
- Other

9.6.3 Data Pool Value-Added Services

Restrictions placed upon Recipient Data Pools that limit how they can handle GDSN Data information sent to and from trading partners would severely hamper the Recipient Data Pool's ability to perform or provide these services for their members. It may also limit the Recipient Data Pool's ability to comply with all of the GDSN Data synchronisation process requirements relating to validations, synchronisation list processing and maintenance and potentially disrupt their ability to support the existing business process of their trading partners.

- GDSN Data applications
- Robust user interface allowing the Data Recipient to enter information directly into the Data Pool
- Workflow processing
- Supplier and/or Retailer specific validations
- Message and file level track and trace for audit or problem resolution
- Reporting
- Retransmission capabilities

- Other

It is important to consider the aspect of Trading Partner Agreements that may be in place.

Today Trading Partner agreements governing data confidentiality and usage may not exist, may not be legally binding, or may be too vague to be of value. This needs to be left up to individual Trading Partners.

Recommendation / Requirement – Strongly encourage Trading Partners to have confidentiality agreements in place (from business and technical perspective) with all business partners, and to include those requirements in these agreement(s).

Appendix E gives a reference to a typical Trading Partner agreement that may be in place today.

This is similar to what is described in Section 5.4.

9.6.4 Data Pool Value Added Services

Any Data Pool value-added services must not expose any part of the GDSN Data to entities or Trading Partners that are neither authorized nor authenticated to receive and / or view the messages or the data contained in the messages.

9.7 Authorisation

The ability to ensure that the entity that is attempting to perform a task is really the entity it says it is. The ability to authorize an entity or a trading partner is instrumental in establishing confidence in the data pool as well as the GDSN itself.

9.8 Access Control

This is the method by which only the entities that have rights and privileges to access and receive the data are the only ones to have access to it. This ability to properly ensure that an entity or a trading partner is allowed to receive or view the messages is also instrumental in establishing confidence in the data pool as well as the GDSN itself.

10 Third Party Audits

10.1.1 Summary

While GDSN nor Trading Partners can act as security 'regulators', GDSN acknowledges and recommends External Third Party audits to validate that the control points and base levels of security are addressed throughout the processes between Trading Partners. These control points and base levels of security are defined by the Trading Partner Agreements which guide the Trading Partner / Data Pool and Data Pool / Data Pool agreements.

10.1.2 Trading Partner Agreements

Today Trading Partner agreements governing data confidentiality and usage may not exist, may not be legally binding, or may be too vague to be of value..

Recommendation / Requirement – Strongly encourage Trading Partners to have confidentiality agreements in place (from business and technical perspective) with all business partners, and to include those requirements in these agreement(s).

Appendix E gives a reference to a typical Trading Partner agreement that may be in place today.

10.1.3 Third Party Audit Discussion Guide

While ISO 17779 and SAS 70 have been widely used and accepted, flexibility is required to accommodate different companies from different parts of the country.

Appendix C and D references ISO 17779 and SAS 70.

A. IMPLEMENTATION CONSIDERATIONS

A.1 Security

- How is physical access to facility controlled? examples: Badges, Guards, CCTV cameras, Perimeter access controls, Internal area controls, Badge logs, Visitor escort policy, Sign-in logs
- How is access to related systems, applications, and networks controlled? Network login, User/ID password, Strong authentication
- Can system, application, and network actions be traced to an individual account and action time? Network logs, system logs, application logs, audited actions, non-audited actions, success audits, failure audits
- How information is (electronic & paper) protected from unauthorized disclosure and modification? What is the Document Retention Policy
 - Electronic: account authorization, account privileges, encryption.
 - Paper: locked offices, locked filing cabinets, locked desk drawers, document classification markings, shredding policies
- Protection of the software code to prevent things like “backdoors” left in the code, etc.
- Global Registry and Data Pool personnel with access to the data, and address Add, Change, Delete actions, download capabilities, printing, disclosure of information, confidentiality, etc. Do organizations have background checking policies and procedures?

Several concerns have been raised by the different parties involved in the communication of GDSN Data information through the GDSN. This list probably does not represent all concerns.

- Trading partners may not want Price Synchronisation data in locations outside the trading partner relationship.
- Trading partners want assurance that the data pools provide access controls that restrict access to the GDSN Data to only the trading partner for whom the data is intended.
- There are current proprietary data pool implementations of additional value-added services that the data pool community will not want GDSN Data synchronisation security to constrain.
- Some trading partners believe some level of encryption may be required. Encryption could include the entire message down to individual tags contained within the message payload. While providing an additional level of security, encryption can also create barriers to how GDSN Data is communicated within the network as well as impediments to the processing that may be required of the data pools.

A.2 Anti Virus

- Does the organization have anti-virus software installed on all related systems? Servers, user desktops, user laptops, user PDA's, email system
- How frequently are the anti-virus software and signature files updated? daily, monthly, quarterly, immediately or "n" days/week after release from vendor

- How frequently is the anti-virus software used to scan for viruses? Hourly, daily, weekly, or on email receipt?
- What level of control for work stations? Can individual users disable any of these key features? Disable or bypass the anti-virus software? Download software, install software? Perform admin level functions?
- What are personnel to do if they detect a virus? Stop using system, contact admin, and remove virus, document date/time and virus type, remove system from network?

A.3 Password & PIN Security

- Is there a password policy? password sharing, protection, password length, complexity and age requirements
- What password length and complexity technical controls are in place? password length enforcement, special numeric enforcement, password age enforcement, password reuse enforcement, invalid attempt thresholds
- Do users use shared accounts? multiple people using one account
- Are default passwords required to be changed?
- What is the process for resetting a password when user cannot remember it? Call helpdesk, visit admin, submit form signed by supervisor etc.

A.4 Network & Computing Resources

- How is access to related systems controlled? Username password, 2-factor authentication, one time password, etc.
- Are any related systems configured for remote access? Remote admin, remote users, modem, VPN, secureID or PKI
- Are related systems connected to any other networks? dual homes systems, internet connectivity, shared networks
- Are employees allowed to use their non-business personal computers to access related systems, or connect to related networks?

A.5 Backups & Disaster Recovery

Questions:

- Are there formal documented backup procedures and schedules that exist in creating copies of: operating system software, system data and security files/tables, production libraries/directories and databases (including program source), development tables, libraries/directories and databases
- What is the backup rotation schedule?
- Is the internal control environment over process clearly defined?
- Is documentation reviewed and updated annually?

- Have internal controls been systematically tested?
- Is testing of the internal controls retained in accordance with record retention?
- Is system and security configuration stored in a secure location on-site?
- Are backup files stored in a secure location onsite?
- Where is the onsite backup storage facility located?
- How long are backup tapes/disks kept onsite?
- Does company have an off-site storage facility?
- Does company have a written contract with off-site storage facility?
- How long does it take to retrieve a backup from an off-site storage facility?
- Backups and disaster recovery
- How often are backups moved to the off-site location?
- Are file and library backups kept at the off-site storage facility? Security files? Operating system? Documentation? Policies and procedures?
- Is a copy of the disaster recovery procedures at the off-site facility?
- Are the backups stored in secured containers while transport to and from the off-site facility?
- Does the company have a current disaster recovery plan?
- Does the plan include a sequence for restoring the systems that takes into consideration the criticality of the system?
- Has the disaster recovery ever been tested? And when?
- Have the test results been documented and followed up for problems?
- Have Information Management (System Support) and user responsibilities related to implementing and testing been defined?
- Have critical business and information assets been defined?
- Has a risk assessment been conducted to identify risks and evaluate the impact to business?

B. COMMENTS FROM GS1 AUSTRALIA

(This section included with permission from GS1 Australia and Task Group)

We are often asked to provide responses to risk assessments from current and/or prospective users of our data pool. Generally a substantial amount the information that is provided in responses to these requests can be sourced from a SAS 70 Type II report. Some prospective users have indicated that unless the vendor is SAS 70 Type II certified, and non-public data is hosted by the vendor outside of their enterprise, an on-site assessment would need to be scheduled.

Additionally it would appear that a SAS 70 Type II certification provides users with the assurances they are looking for whereas a SAS 70 Type I is not considered to be adequate. It should be noted however is that a SAS 70 report focuses primarily only on the infrastructure associated with the service organisation and do not typically cover Application Security. In our experience it is the absence of any assessment and assurances associated with the security of the application itself that a SAS 70 report alone may fall short in addressing the needs and concerns of many prospective users.

Therefore we find that from an ongoing governance perspective that we need to also undertake additional independent 3rd party security assessments are required in order to demonstrate overall application/service security. These 3rd party assessments are able to leverage the existing information that is available in SAS 70 reports and then build upon that information to provide a more complete assessment.

Typically, users are seeking assurances with respect to the following aspects of security;

1. Physical Security
2. Network Security
3. Systems Security
4. Application Security

C. SAS 70

Much of the information in this section is based on the American Institute of Certified Public Accountants (AICPA) audit guide entitled "Service Organizations, Applying SAS No. 70, As Amended".

C.1 SAS 70 Overview

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS No. 70 is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centers, Internet data centers, or other data processing service bureaus.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit as required in SAS No. 55, Consideration of Internal Control in a Financial Statement Audit. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at the service organization.

C.2 Service Auditor's Reports

One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report are described in the following table:

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

C.3 Benefits to the Service Organization

Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors

can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

C.4 Benefits to the User Organization

User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

User organizations should provide a Service Auditor's Report to their auditors. This will greatly assist the user auditor in planning the audit of the user organization's financial statements. Without a Service Auditor's Report, the user organization would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures.

D. ISO 17799

D.1 Overview

ISO17799 is actually "a comprehensive set of controls comprising best practices in information security". It is essentially, in part (extended), an internationally recognized generic information security standard.

Its predecessor, titled BS7799-1, has existed in various forms for a number of years, although the standard only really gained widespread recognition following publication by ISO (the International Standards Organization) in December of 2000. Formal certification and accreditation were also introduced around the same time.

D.2 The Contents of the Standard

The ISO 17799 standard comprises ten prime sections:

1. Business Continuity Planning

The objectives of this section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control

The objectives of this section are: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorised activities. 6) To ensure information security when using mobile computing and telenetworking facilities

3. System Development and Maintenance

The objectives of this section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data.

4. Physical and Environmental Security

The objectives of this section are: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

5. Compliance

The objectives of this section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security

The objectives of this section are: To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organisation

The objectives of this section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties. 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Operations Management

The objectives of this section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimise the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; 7) To prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

The objectives of this section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are: To provide management direction and support for information security.

Within these sections are the detailed statements and clauses that comprise the standard itself. In addition, the standard includes a Forward (setting the scene), a Scope, and a section defining various terms.

D.3 Certification and Compliance

The first step towards ISO 17799 certification is of course to comply with the standard itself. This is good security practice in its own right, but it is also the longer term status adopted by a number of organizations, who require the assurance of an external measure, yet do not wish to proceed with an external or formal process immediately.

In either case, the method and rigor enforced by the standard can be put to good use in terms of better management of risk. It is also being used in some sectors as a market differentiator, as organizations begin to quote their ISO 17799 status within their individual markets and to potential customers.

There is no doubt that ISO17799 is not going to disappear - far from it. Whatever your intention, however, it is hoped that this Directory will assist. You can directly acquire not only the standard itself or the accompanying introductory toolkit, but software to help with compliance, ISO 17799

aligned security policies, a risk analysis product (risk assessment is actually a basic requirement of the standard) and a number of other essential resources.

E. SAMPLE EXISTING TRADING PARTNER TO TRADING AGREEMENT

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

THIS ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT (the "Agreement") is made as of [***], 19[***], by and between _____ Corp. ("_____"), a Delaware corporation, with principal offices at _____ and [***] ("Company"), with principal offices at [***].

RECITALS

_____ and Company desire to facilitate purchase and sale transactions ("Transactions") by electronically transmitting and receiving data in agreed formats in substitution for conventional paper-based documents and to assure 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.

NOW THEREFORE, the parties, intending to be legally bound, agree as follows:

Section 1. Prerequisites.

1.1. Documents:Standards. Each party may electronically transmit to or receive from the other data in agreed formats ("Documents"). Any transmission of data which is not a Document shall have no force or effect between the parties unless justifiably relied upon by the receiving party. All documents shall be transmitted in accordance with the standards, ANSI ASC X12 as published by the American National Standards Institute, Accredited Standards Committee X12.

1.2. Third Party Service Providers.

1.2.1. Documents will be transmitted electronically to each party either directly or through any third party service provider ("Provider") with which either party may contract. Either party may modify its election to use, not use or change a Provider upon 30 days prior written notice.

1.2.2. Each party shall be responsible for the costs of any Provider with which it contracts.

1.2.3. Each party shall be liable for the acts or omissions of its Provider while transmitting, receiving, storing or handling Documents, or performing related activities, for such party; provided, that if both the parties use the same Provider to effect the transmission and receipt of a Document, the originating party shall be liable for the acts or omissions of such Provider as to such Document.

1.3. System Operations. Each party, at its own expense, shall provide and maintain the equipment, software, services and testing necessary to effectively and reliably transmit and receive Documents.

1.4. Security Procedures. Each party shall properly use security which such party reasonably believes to be sufficient to ensure that all transmissions of Documents are authorized and to protect its business records and data from improper .

1.5. Signatures. Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained in each Documents transmitted by such party ("Signatures"). Each party agrees that any Signature of such party affixed to or contained in any transmitted Document shall be sufficient to verify that such party originated such Document and neither party shall contest the validity or enforceability of the document on this basis. Neither party shall disclose to any unauthorized person the Signatures of the other party.

Section 2. Transmissions.

2.1. Proper Receipt. Documents shall not be deemed to have been properly received, and no Document shall give rise to any obligation, until able to the receiving party at such party's receipt computer.

2.2. Verification. Upon proper receipt of any Document, the receiving party shall promptly and properly transmit a functional acknowledgment in return. A functional acknowledgment shall constitute conclusive evidence a Document has been properly received.

2.3. Acceptance. Any such Document which has been properly received shall not give rise to any obligations unless and until the party initially transmitting such Document has properly received in return an acceptance Document.

2.4. Garbled Transmissions. If any transmitted Document is received in an unintelligible or garbled form, the receiving party shall promptly notify the originating party (if identifiable from the received Document) in a reasonable manner. In the absence of such a notice, the originating party's records of the contents of such Document shall control.

Section 3. Transaction Terms.

3.1. Terms and Conditions.

3.1.1. Prices, any additional charges, payment terms, delivery, and shipping will be set in accordance with the then current written agreement between _____ and Company. In the absence of any other written agreement applicable to any Transaction made pursuant to this Agreement, such Transaction (and any related communication) also shall be subject to such additional terms and conditions as may be determined in accordance with applicable law.

3.1.2. If this Agreement is incorporated into another agreement between the parties, in the event of any conflict between the terms of this Agreement and such other agreement, except as otherwise expressly set forth in such other agreement, the terms and conditions of this Agreement shall govern.

3.1.3. Each party will generate Transactions in accordance with the applicable terms and/or laws. In the event that such purchase orders do not comply with the terms and/or laws set as provided above, the receiving party will notify The other party of the discrepancy and Such other party will thereafter either transmit transaction changes or enter the order without the use of EDI. Transactions involving amounts in excess of \$_[***]_____ will also be entered without the use of EDI.

3.2. Confidentiality. Except to the extent provided in Section 1.5, by written agreement between the parties, or by applicable law, no information contained in any Document or otherwise exchanged between the parties shall be considered confidential. Nevertheless, the parties shall exercise reasonable care to prevent such information from being misdirected or otherwise disclosed to any other person.

3.3. Validity; Enforceability.

3.3.1. This Agreement has been executed by the parties to evidence their mutual intent to create binding purchase and sale obligations pursuant to the electronic transmission and receipt of Documents specifying certain of the applicable terms.

3.3.2. Any Document properly transmitted pursuant to this Agreement shall be considered, in connection with any Transaction, any other written agreement described in Section 3.1, or this Agreement, to be a "writing" or "in writing"; and any such Document when containing, or to which there is affixed, a Signature ("Signed Documents") shall be deemed for all purposes (a) to have been "signed" and (b) to constitute an "original" when printed from electronic files or records established and maintained in the normal course of business.

3.3.3. The conduct of the parties pursuant to this Agreement, including the use of Signed Documents properly transmitted pursuant to this Agreement, shall, for all legal purposes, evidence a course of dealing and a course of performance accepted by the parties in furtherance of this Agreement, any Transaction and any other written agreement described in Section 3.1.

3.3.4. 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. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of Signed Documents under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Signed Documents were not originated or maintained in documentary form.

Section 4. Miscellaneous.

4.1. Termination. This Agreement shall remain in effect until terminated by either party with not less than thirty (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 Documents or otherwise under this Agreement prior to the effective date of termination.

4.2. Severability. Any provision of this Agreement which is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

4.3. Entire Agreement. This Agreement constitutes the complete agreement of the parties relating to the matters specified in this Agreement and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either party. No obligation to enter into any Transaction 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.

4.4. Assignment. Neither party has the right to assign this Agreement in whole or in part without the prior written consent of the other except that either party may make such an assignment to another corporation wholly-owned by or under common control with it. For

purposes hereof, the term "assign" will include, without limitation, a merger, sale of assets or business, or other transfer of control by operation of law or otherwise.

4.5. Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the State of Illinois, U.S.A., excluding the provisions thereof relating to conflicts of laws.

4.6. Force Majeure. No party shall be liable for any failure to perform its obligations in connection with any Transaction or any Document, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

4.7. Limitation of Damages. Neither party shall be liable to the other for any 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 Documents pursuant to this Agreement, even if either party has been advised of the possibility of such damages.

4.8. Arbitration. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled in accordance with the Commercial Arbitration Rules of the American Arbitration Association, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

Each party has caused this Agreement to be properly executed on its behalf as of the date first above written.

_____ Corp.
 By: _____
 Name: _____
 Title: _____
 Date: _____

Company
 By: _____
 Name: _____
 Title: _____
 Date: _____