GDSN Security Audit Requirements

Issue # 1, 01 December 2011

Document Summary

Document Item	Current Value
Document Title	GDSN Security Guidelines
Date Last Modified	01 December 2011
Current Document Issue	Issue # 1
Status	Approved
Document Description	GDSN Security Audit Requirements Document

Contributors

Name	Organization
GDSN Operational & Technology Advisory Group	GS1

Log of Changes in Issue

Issue No.	Date of Change	Changed By	Summary of Change
1	01December2011	Sean Lockhead	Creation of Version 2.0 Document

Disclaimer

Whilst every effort has been made to ensure that the guidelines to use the GS1 standards contained in the document are correct, GS1 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

1.1. Introduction

With strong commitment to the vision and principles of Global Data Synchronisation, it is recognized that in order for this vision to be achieved, standard, compliant information must be able to flow uninterrupted between trading partners in a secure fashion. Data to support the exchange of supply chain information can include price information, which is the most sensitive of all data. Not only does it carry the greatest risk when not handled securely, but it also carries the greatest rewards when handled securely.

One of the key considerations for ensuring the usability and wide adoption of the Global Data Synchronisation Network (GDSN) is the security required to run an interactive network. Responding to concerns expressed both from the community and the industry at large, GDSN has collaborated on these requirements which address all aspects of security (physical, logical, business processes and contractual).

This document describes the GDSN requirements for addressing a security audit within the GDSN network as well as beyond the network to include recommendations for the relationship between Source / Recipient Data Pools and Data Source / Data Recipients.

It is the position of GDSN that Trading Partner agreements ultimately govern and drive the Supplier and Retailer relationship and their associated relationships with their Data Pools. As such, Trading Partners must have legally enforceable agreements in place where data ownership and security are concerned.

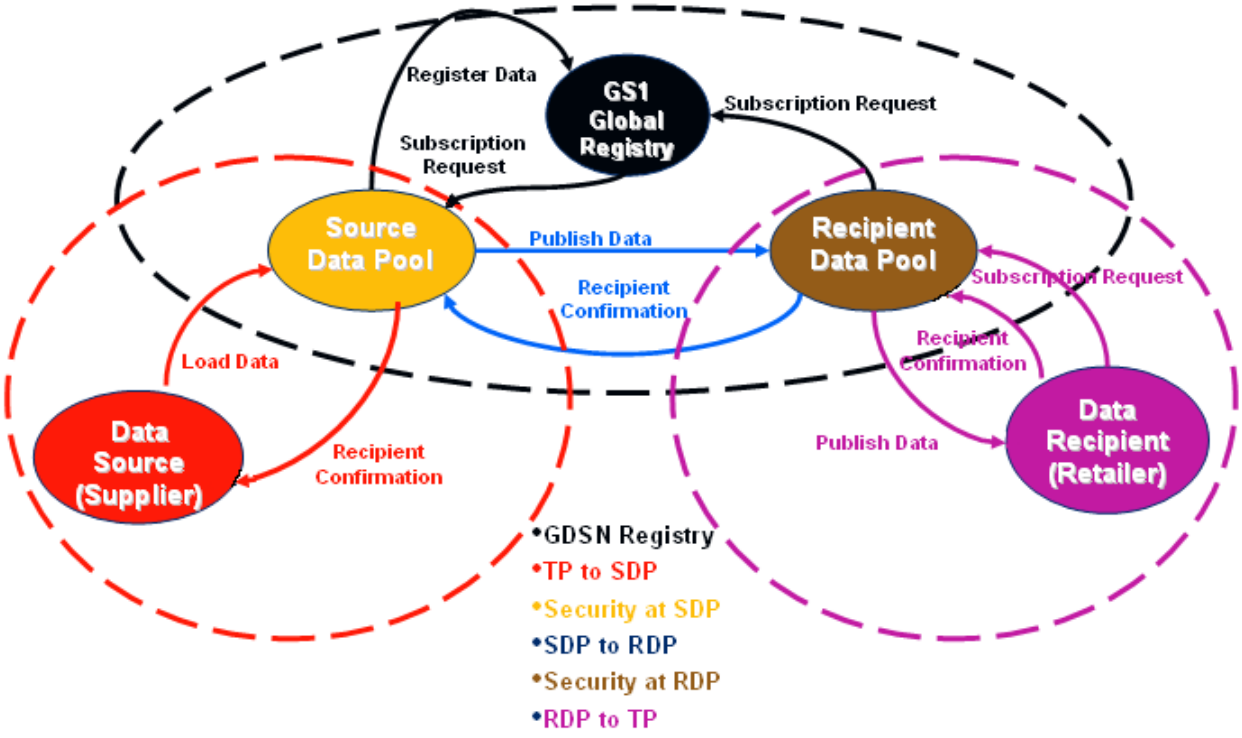
This security audit requirements document is intended to examine the breadth and depth of a security audit, the various components involved and the requirements or recommendations, depending on whether in, or out of the network.

The goal of the Security Audit is to ensure the confidence of the Data Source / Data Recipient that the storage and handling of their GDSN data is secure at all times through the process both in / out of GDSN network. Actual enforcement by GS1 GDSN, Inc. is restricted to GDSN processes. As such, security audits must be addressed at several levels within and throughout the process which includes participants beyond the GS1 Global Registry®, beginning with the Data Source, to the Source Data Pool, to the Recipient Data Pool, and finally the Data Recipient. Depending on the point in the process, different solutions, measures and / or controls will be required to ensure security of the data.

The information contained in this document represents the current view of GS1 GDSN, Inc. and may be changed over time as technology; security best practices and supply chain automation evolve.

1.2. Choreography

GDSN CHOREOGRAPHY



1.3. Relationship Scenarios

Companies have an almost limitless variety of options on how to manage their Information Technology (IT) infrastructure. The structure utilized by an organization impacts their security needs and audit requirements. For example; in the simplest scenario, a Company owns all IT assets, operates these in a facility they own and manage, plus controls all the administration of the applications.

Following is a list of common options used by organizations to manage IT infrastructure:

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

Due to the constant reallocation of scarce resources, many large companies utilize a combination of all of the above models. With the advent of telecommuting, Wi-Fi hotspots, Virtual Private Networks (VPN), use of personally owned computers, etc., IT networks have increased in complexity. This complexity frequently causes the ownership of IT assets difficult to discern, even to members of the organization's IT department.

2. Common Elements

2.1. GDSN Data

GDSN Data can be viewed as Party, Catalogue Item, Price, or any other information that is communicated in the Global Data Synchronisation Network (GDSN). The processes for the dissemination of this information are related but not truly interchangeable. These security requirements address both the similarities as well as the differences.

2.2. Transport Protocols

In the GDSN, the only transport protocol is the use of Electronic Data Interchange over the Internet, Applicability Statement 2 (EDIINT AS2). This is a mandatory requirement for Data Pools and the GS1 Global Registry® in the GDSN.

For additional information, please refer to EDIINT AS2 document and GS1 GDSN, Inc. Operations Manual.

2.2.1. Encryption

Encryption is critical part of secure data handling. GDSN utilizes AS2 encryption. Beyond GDSN, there can be other types/levels of encryption with various benefits and constraints that should be assessed by the users. Examples of additional encryption are:

- Transport Protocol Message encryption (AS2)
- Data (Payload) Encryption
    - Full – Encryption of entire payload – Requires additional content.
    - Partial – Encryption of certain individual attributes value(s) within the payload.

Note: Encrypting attribute values are above and beyond the current scope of GDSN and would only be recommended if the function is needed.

Data messages communicated between all parties in the GDSN network will by encrypted by the use of EDIINT AS2 protocol.

There are no standards governing the storage of data by Data Pools or the communication between the Data Pools and their Trading Partners. Internal storage and encryption of data is based on the business relationship between the Data Pool and its Trading Partners. For example, Price security obligations may be managed by the mutual agreement of the Data Pool and its members.

2.2.2. Digital Certificates

Certified Data Pools must use a self-signed certificate or a signed digital certificate from a recognized third party organization that is responsible for the issuance of these types of certificates. All Data Pools and the GS1 Global Registry® must implement the use of digital certificates and maintain an up-to-date listing of all the other Data Pools and GS1 Global Registry® digital certificates.

Use of an additional digital certificate between a data pool and its trading partners should be handled within their relationship agreement. Refer to the GS1 GDSN, Inc. Operations Manual in regards to any additional digital certificate information or AS2 information.

2.3. GDSN Data Ownership

To properly address security issues and concerns as they relate to the data pools, the major issue that must be addressed and resolved is 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.

Generally, the retailer owns the rights to distribute the data they received from the supplier. This is typically governed by the terms of a trading partner agreement. It is also assumed retailers can store data in any form they prefer, if it is satisfactory to mutual agreements with suppliers and if it does not violate GDSN standards.

One of the most interesting questions for security of data is who is responsible for the data as it passes through transactional messaging systems that span several business entities and boundaries. When a source gives permission to a source data pool to send GDSN Data information to a recipient, the information is sent to the recipient for their use. Does that data belong to the recipient? This issue is typically mediated by a trading partner agreement between the supplier and the retailer. This agreement should outline the responsibility of each party and the terms of use and confidentiality governing the data. If trading partners agree on the use and security and confidentiality surrounding the information to be shared, then the trading partner agreements that exist with each of the service providers involved between the trading partners must include a provision that each provider will be held to the same or more stringent security measures and confidentiality.

With messages transmitted across the GDSN, normally the following assumptions exist:

- The trading partner agreements between the Data Source, their Source Data Pool and their trading partners govern the data ownership, confidentiality and responsibilities of the GDSN information.

- 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 Recipient is responsible for controlling what actions may be taken with the data and protecting the confidentiality of the data.

Additional issues that should be considered by Trading Partners as a result of the preceding assumptions are as follows:

- The ramifications of the retailer receiving data and taking ownership of the data upon receipt from supplier
- Agreements that must be in place to allow entities to use or host the transmitted data on a secured site (web portal) for the use of their user community (individual stores, users).
- If GDSN data can be hosted by a Retailer and placed on a Retailers web portal, hosted by third party.
- If the hosted solution with GDSN Data information is outsourced, there may be additional agreements that need to be in place to protect the confidentiality of the data.
- Any mutual agreements between supplier and retailer that govern what kind of third party is allowed to host the retailer's solution.

As previously stated, once the retailer receives the data, they can communicate or make it available to their own users in any method/format they prefer.

3. GDSN Registry

3.1. Summary – GS1 Global Registry

The GS1 Global Registry® is responsible for ensuring that trading partners are registered at the GS1 Global Registry® (members of GDSN), and have passed the GDSN-mandated validations. Through the use of the Basic Party Synchronisation process, the GS1 Global Registry® communicates all validated Trading Partners (GLN's) to all Data Pools for use in the GDSN Business Message Standard use cases.

The GS1 Global Registry® is responsible for ensuring that registry transactions (Item, Party, Subscriptions etc.) processed at the GS1 Global Registry® have passed the GS1 Global Registry® specific GDSN-mandated validations and have been submitted by registered, validated Parties (GLN). Through the use of the Catalogue Item Synchronisation process, the GS1 Global Registry® enables Data Pools to communicate standards-based business messages for all use cases.

The GS1 Global Registry® Item / Subscription matching process functionally provides data pools and trading partners the information necessary to perform GDSN use cases. The GS1 Global Registry® distributes subscriptions to one or more data pools with registered items that can fulfill the subscription criteria. Through the use of the Catalogue Item Synchronisation process, the GS1 Global Registry® enables data pools to communicate the standards-based business messages for all the use cases.

3.2. Physical

3.2.1. Database

Access to the GS1 Global Registry® is restricted to authorized personnel of the GDSN Development, Hosting, and Customer Service providers. These functions may be outsourced to a technology service provider by GS1 GDSN, Inc.

Data access types for GS1 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

3.2.2. Messaging

The GDSN makes use of the Electronic Data Interchange over the Internet Applicability Statement 2 protocol (EDIINT AS2).

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 dispatched to the appropriate processor based upon its content-type.

As part of the EDI INT messaging, the use of digital certificates is mandated in the Global Data Synchronisation Network. The exchange of the digital certificates is facilitated by the GDSN Customer Support Group.

3.3. Compliance

The GS1 Global Registry® must successfully complete all certification events and remain certified for participation in the GDSN.

3.4. Legal

The GS1 Global Registry® is required to meet or exceed the Service Levels set forth in the GS1 GDSN, Inc. Statement of Work for the GS1 Global Registry® Service Provider. (Refer to SLA definitions).

3.4.1. Service Level Agreements (SLA)

- It is the responsibility of the GS1 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 that is stored in the Global Registry.
- The function of setting up the Data Pools in the GS1 Global Registry® falls to the GDSN Customer Support Staff, operating under the direction of GS1 GDSN, Inc. and in unison with the GS1 Global Registry® provider.
- The GS1 Global Registry® is required to process all valid messages. It is agreed that scheduled outages, which have been communicated by the GS1 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).

3.5. Communication within the GDSN

The trading relationship between the GS1 Global Registry® and the Data Pools covers how the data is communicated between network entities.

Please refer to GRALA (GS1 Global Registry® Access and License Agreement) for additional information.

3.5.1. Data Communication

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

3.6. Trading Partner Security Requirements

Following are GDSN Trading Partners requirements for information registered in the Global Registry:

- Trading Partners must be satisfied that any information registered in the GS1 Global Registry® (parties, items, subscriptions) is only accessible by authorized entities.
- Data Pools and Trading Partners require information that is communicated to and from the GS1 Global Registry® to each entity be secured from an access-control as well as an authorization perspective.

Note: As new functionality is added to the Global Registry, additional requirements may evolve.

3.7. GS1 Global Registry® Security Requirements

The Security Audit process ensures that the GS1 Global Registry®, at a minimum, demonstrates the following:

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

- Adequate access controls are in place to ensure data is exposed and distributed only to the appropriate Data pools.

4. Trading Partner to Source Data Pool

4.1. Summary

Source Data Pools have the ultimate responsibility for the communication of GDSN Data into the Global Data Synchronization Network (GDSN). They are responsible for; gathering GDSN Data from their supply side trading partners, performing validations upon the data, registering items in the Global Registry, managing that the data is sent to the correct trading partner or their GDSN-certified RDP and for ensuring the data is compliant when distributed into the network. This section of the Security Audit explains the role of the Source Data Pool, highlighting the issues and concerns related to Source Data Pools and their relationships with their trading partners.

4.2. Communication of Synchronization 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 the additional value-added services they perform for those members. These relationships also cover what transport protocol is utilized with the trading partner.

Additional value added services that performed by Source Data Pools could include; additional data validations, transformation of the data from different formats, use of the data within other applications, and many others. A Security Audit should embrace these service areas for requirements gathering.

4.2.1. 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 services for their members and therefore should be avoided. Restrictions may also limit the Source Data Pool's ability to comply with all of the GDSN Data synchronization process requirements relating to validations, synchronization list processing or maintenance and, potentially disrupt their ability to support the existing business process of their trading partners.

Following are examples of Data Pool valued added services:

- 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

A Security Audit should also address valued added service areas during requirements gathering.

4.3. Trading Partner Security Audit Requirements

Below are Trading Partner requirements for communication of GDSN information. All of these should be addressed by the audit processes and procedure definition.

- Suppliers are concerned that they only have trading agreements with their own Source Data Pools and their Data Recipients, but not the intervening Recipient Data Pools. Suppliers want insurance that there security requirements are meet by Recipient as well as Source Data Pools.
- Both the Retailers and Suppliers want assurance that the data pools provide controls that restrict access to GDSN Data to only the trading partner for whom the data is intended.
- GDSN Data synchronization should not constrain proprietary data pool implementations of additional value-added services.
- Some trading partners believe a minimum level of encryption must be maintained. This could include encryption of the entire message down to individual tags contained within the message payload. If encryption is utilized, it cannot create barriers as to how GDSN Data is communicated within the network, nor to the data processing that may be required by data pools.
- Data Pools must demonstrate the successful completion of a third party administered security audit.
- Adequate access controls must be in place to ensure data is exposed only to the appropriate data recipients.

5. Security at Source Data Pool

5.1. Summary

This document describes the strategy for addressing security audits of GDSN Source Data Pools (SDP) 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 aspects of security audits that need to be addressed. These are covered in this section.

5.2. Data Stored vs. Data Passed

An issue often raised by suppliers is a requirement that data not reside on the data pool but only pass to recipients. As required by the GDSN design, all data, even 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 stored for the very short time.

There are potential ways to provide for a pass-through mechanism. For example, one possible solution is to encrypt the part of the message (for example, Item Price Type Segment) so that the data pool can perform validation and distribution of GDSN Data, and only the intended recipient can read price values and retrieve the information that is intended solely for them.

A GDSN Security Audit Process analyzes the data storage and passage capabilities for the Source Data Pool.

5.3. SDP Security Concerns

The Data Sources (suppliers) may not have agreements with all solution providers used by retailers. In the case of GDSN, these solution providers can be Recipient Data Pools as well as other types of solution providers, as used by the data recipient. The supplier can have a mutual agreement with the retailer regarding their data and the use of this data by retailer's contracted solution providers. If the supplier is not comfortable with the solution and processes used by the rRetailer, they can opt to use either peer to peer solutions or other processes outside the GDSN.

The basic role and behavior of the data pool in the GDSN is clearly defined. Data Pools also may provide value-added services to its members outside of the network.

A Security Audit is necessary to perform checks for these types of relationships.

5.4. Conclusion

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

Additional requirements may be added to the legal GDSN data pool agreement (GRALA) stating that Data Pools agree to make data available only to the designated party. If the data recipient is a member of another data pool, only the designated data pool would get the data (i.e. a SDP can only guarantee that the data has been delivered to a RDP).

6. Security from SDP to RDP

6.1. 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. When information is exchanged, Certified Data Pools communicate using, GDSN standards-based processes between Source Data Pool and Recipient Data Pool.

6.2. GDSN Certification

All Data pools operating in the Production GDSN environment, where all the live synchronisation processes occur, must pass the GDSN Certification Process as defined by GS1 GDSN, Inc. There is limited certification criteria that impacts the overall security of the GDSN, as most of the certification concentrates on the functionality.

6.3. SDP to RDP Security Concerns

6.3.1. Priority / Applicability of Multiple Agreements

Security audits needs to ensure that there are no conflicts between multiple agreements and that the security audit process account for multiple agreements.

The security audit needs to establish a clear line of precedence (and priority) for agreements so that there are no conflicts between multiple agreements exist. Examples of multiple agreement structures are as follows:

1. Non GDSN DATA POOL – DATA POOL in GDSN
2. Non GDSN DATA POOL –Non GDSN DATA POOL
3. TRADING PARTNER – DATA POOL in GDSN
4. TRADING PARTNER – TRADING PARTNER

7. Security at Recipient Data Pool

7.1. Recipient Data Pool Role

The role of the Recipient Data Pool (RDP) in the Global Data Synchronization 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. The RDP receives GDSN standard messages from Source Data Pools, plus the GS1 Global Registry®. The RDP routes the messages only to the recipients designated in the messages which could include third parties outside the network.

7.2. Recipient Data Pool Security Audit Requirements

7.2.1. Established Relationships

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 with the data recipient responsible for the 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 area for the Data Recipient's data and for reloads of the data should a failure happen in the recipient's internal data repository. All processing should be based on a mutually-agreeable timeframe and not impact or take precedence over the agreements between the Data Source and the Data Recipient and the Trading Partner and its Data Pool.

When there are multiple relationships, the security audit of the data and processes must ensure that the requirements are met through all relationships. With the above described scenario, the first relationship is a trading partner relationship. This is an agreement between the trading partners and it will govern the use of and confidentiality of the data in the relationship. A trading partner agreement can be executed that describes the use of data, by whom, for what and the penalties for breaches to the contracted use of data. A security audit must be strategically defined for this relationship.

The second relationship for the above scenario is between the recipient trading partner and its data services provider. In this relationship, the recipient needs to hold 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 source and recipient, all responsible for upholding / maintaining integrity and security of the data. This will include but may not be limited to; GDSN recipient data pool(s) applications, 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 should be limited specific requirements in terms of technology platform considerations.

8. Security from Recipient Data Pool to Data Recipient

8.1. Summary

Message information at the 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.

8.2. Communication of Synchronization 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 requirements cover 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. A Security Audit should embrace these service areas for requirements gathering.

8.2.1. 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 synchronization process requirements relating to validations, synchronization list processing and maintenance and potentially disrupt their ability to support the existing business process of their trading partners.

Examples of some Data Pool valued added services are as follows:

- 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

The Security Audit Process is strategically defined to address this type of relationship and not constrain nor force a particular implementation methodology in this setting.

8.3. Authorisation

Authorisation is 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 authorise an entity or a trading partner is instrumental in establishing confidence in the data pool as well as the GDSN itself.

A Security Audit needs to ensure the ability to perform the authorisation function.

8.4. 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.

A Security Audit needs to ensure the ability to perform the access control function.

9. General GDSN Security Audit Requirements

9.1. Audit Discussion Guide

9.1.1. Functional / Technical

Requirements for a Security Audit should take into consideration:

- How code is developed (processes)
- Open access to source code
- Personnel involved in any of the areas of the GDSN (DS, SDP. GR, RDP, DR)
- Functional – to be defined as functional developed
- Frequency – Consistency with currently implemented industry guidelines

9.1.2. GS1 Global Registry® Impact

GS1 GDSN, Inc. outsources development, hosting and customer support to Summa Technology Group. The GS1 Global Registry® is managed through Summa and is currently hosted at Internap who has passed the SAS70 Type II Audit. The introduction of the Service Auditors to the Statements on Standards for Attestation Engagements No. 16 (SSAE 16), (Service Organization Control (SOC) reporting options – SOC 1, SOC 2 and SOC 3) became effective in June 2011. Intermap's final SAS 70 audits were completed covering a period of October 1, 2010 thru March 31, 2011. In November 2011, Intermap issued new SOC 2 audit reports which are available to its customers. The new reports cover the audit period April 1, 2011 thru September 30, 2011.

As additional GDSN audit requirements are gathered, the current GS1 Global Registry® audit will be evaluated as to the best scenario to meet any new security audit requirements.

9.1.3. Data Pool

Relationships can exist between trading partners and these must be covered contractually. Each individual trading relationship must be analyzed to determine how they do business and the viability of a GDSN Security Audit solution. Additional Data Pool to Trading Partner agreements must cover 3rd parties as well as 3rd party to other retailers.

9.2. Audit Questions

This section details questions that should be answered during the security audit. These questions cover; General Security, Anti-Virus Measures, Password & Pin Security as well as Network & Computing Resources.

9.2.1. General Security

- How is physical access to the 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 is information (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
- What are the procedures to protect software code to prevent things like “backdoors” left in the code, etc.?

9.2.2. 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?

9.2.3. 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.

9.2.4. 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?

9.2.5. Backups & Disaster Recovery

- Are there formal documented backup procedures and schedules that exist for 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?
- 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 systems that takes into consideration the criticality of the system?
- Has the disaster recovery ever been tested and how often?
- 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?

10. External Audit Systems

GS1 GDSN, Inc. is aware that there are a number of Auditing Specifications that can be considered for use for a system Audit such as, SAS 70 (being replaced by SSAE 16), ISO 17799, and ISO 27000. It is not the intent of GS1 GDSN, Inc. to mandate a specific audit process but to provide the requirements of an audit for the best overall security of the GDSN. It is a decision of the Data Pool to choose the specific audit that best meets their needs and the GDSN the audit requirements.