INFORMATION TECHNOLOGY

VOLVO

DMS Volvo Gateway Service Technical Specifications

Volvo Financial Services, North America

North American Transaction Services

(NATS)

Version: 1.2

Issuer: Wendy Mendenhall and Bert Wilson

Date: 12/03/2012

Document Versions:

Date	Version	Modified By	Modification Description
8/6/2012	1.0	Bert Wilson	Final document
8/31/12	1.1	Bert Wilson	Updated UAT/Production Gateway URL Minor edits
12/03/12	1.2	Bert Wilson	Updated UAT/Production URLs

1.0 Introduction

The MVPreferred system was created to allow NORTH AMERICAN TRANSACTION SERVICES (NATS) and *VOLVO TRUCKS NORTH AMERICA (VOLVO)* to offer customer preferred pricing from within the existing *DEALER MANAGEMENT SYSTEMS (DMS)*.

This document outlines the required specifications for the security layer in order to pass messages between the DMS and MVPreferred to obtain in *REAL TIME* both the pricing verification and current credit line (*AUTHORIZATION AND SETTLEMENT*) for a fleet client. The process is to allow a DMS to interface with MVPreferred will be via *EXTENSIBLE MARKUP LANGUAGE (XML)* over *HYPERTEXT TRANSFER PROTOCOL (HTTPS)* via the public Internet using *SECURITY TOKEN*.

This document assumes that the reader is well versed in *TCP/IP* communications using various methods and protocols which are readily available via commercial off the shelf products or included with most Operating Systems.

1.1 Summary of Contents of Document

The following conventions are used throughout this document:

- *Capitalized Italics* words (only capitalized the first time) are defined in the Glossary.
- [NOTES: are used to further clarify the discussion or to offer additional suggestions and/or resources wherever applicable].

1.0 Introduction 2
1.1 Summary of Contents of Document 2
1.2 Audience and Scope 3
1.3 Related Documents 3
2.0 System Objectives 4
3.0 Assumptions 5
4.0 Gateway Service 5
4.1 URL address for the Gateway Service 5
4.2 Gateway Service Flowchart 6
4.3 Gateway Service Security Level 7
4.3.1 Security Level 1 7
4.3.2 Security Level 2 7
4.3.3 Security Level 3 7
4.3.4 Security Level Flowchart 8
4.4 XML Get Security Token Request (DMS to MVPreferred) 9
4.5 XML Get Security Token Response (MVPreferred to DMS) 9
4.6 Get Security Token Request - Samples 9

4.6.1 Get Security Token Request Sample XML 9
4.6.2 Get Security Token Request XML Schema 9
4.7 Get Security Token Response - Samples 10
4.7.1 Get Security Token Response XML 10
4.7.2 Get Security Token Response XML Schema 10
5.0 Return Status Codes and Messages 11
6.0 Service Level Agreement 13
7.0 Glossary 13

1.2 Audience and Scope

This document is intended to discuss at a high level, the technical programming requirements to pass the Security Token between two (2) different Operating Systems. The DMS can be any type of computer and operating system and resides at a Volvo/Mack Truck Dealership. MVPreferred resides within Volvo Financial Services LAN Admin Operations Center. The DMS vendors will interface with MVPreferred through the web based exchange process.

Secondary audiences include, but are not limited to: software implementers, quality assurance personnel, and technical writers.

1.3 Related Documents

Documents to integrate DMS with MVPreferred:

1. DMS Volvo Gateway Service tech specs
2. DMS Volvo Price Verification Message Protocol tech specs
3. DMS Volvo Authorization Message Protocol tech specs
4. XML DMS Volvo Batch Invoice Settlement tech specs

2.0 System Objectives

The DMS/MVPreferred messaging system is quite simple in that two (2) different infrastructures (both hardware and Operating Systems) wish to exchange information. The MVPreferred infrastructure is Microsoft Windows 2008 Servers. Client Certificate Authentication certificates will be shared between VFS and the DMS to be added to the web server environment for additional point-to-point security. The transport protocol for messaging will be synchronous messaging over standard HTTPS. The DMS will initiate an HTTPS request to get security token and wait for the response from the MVPreferred, then initiate HTTPS requests with the security token. All other information to be exchanged between the two (2) systems will be via the standard *Secure File Transfer Protocol (SFTP) with encryption*. It will be the responsibility of the DMS to *PUSH* and *PULL* the SFTP files to be exchanged.

- The current DMS *GRAPHICAL USER INTERFACE (GUI)* displays a form for dealer personnel to create an invoice or repair order
- Once all the information has been captured, the dealer personnel will submit the form to MVPreferred for pricing verification
- MVPreferred will interrogate the Volvo database which contains all information required to verify that a client has or does not have preferred pricing for various VOLVO *PART NUMBERS*, and return the information along with status messages
- The DMS GUI will extract any new pricing and adjust the form to reflect the preferred pricing for each of the part numbers.
- A Sales Order Invoice or Repair Order can be presented for Authorization at any time (See SLA for maintenance windows and Authorization and Settlement Technical Specifications for more detail).
- Authorized sales invoices will be batched and sent from the DMS to MVPreferred on a scheduled basis for Settlement and Payment.

3.0 Assumptions

- Use XML over HTTPS - Price verification and Authorization Request coming over public network (HTTPS) with security token returned from Gateway Service.
- Client Certificate Authentication certificates loaded in VFS and DMS webserver environments for point-to-point security
- A sales order invoice authorization request assumes that the DMS has performed all Price Verification prior to Authorization and that the dealership has not changed any prices or added any new line items since the last Price Verification Request.

  NOTE: During Settlement, a final Price Verification will be performed and any price discrepancies will cause that invoice to be rejected. The dealer will be notified of the invoice in question via the Acknowledgement File, and the dealer must correct the invoice via the Invoice Management Pro in the MV Preferred Dealer Portal. The Settlement file will once again flow through normal processing for resubmission for payments. **Price Verifications may be invalid if settlement has not been processed the same day as the authorization code is received.**

- **VFS IT DMS/Dealer network SLA:** the bandwidth and/or availability of the DMS and/or dealers connection from their respective Internet Service Provider is not in scope for VFS IT support
  - VFS IT SLA support covers incoming/outgoing connections to the Gateway Service designated in the specification

4.0 Gateway Service

The Gateway Service is a security layer around the Price Verification and Authorization web services which requires the Price Verification Request and Authorization Request web services to have a token. The DMS requests the token with a call to the GetSecurityToken method and receives a token and token expiration. The same token can be used with the Price Verification Request and Authorization Request as long as the token has not expired.

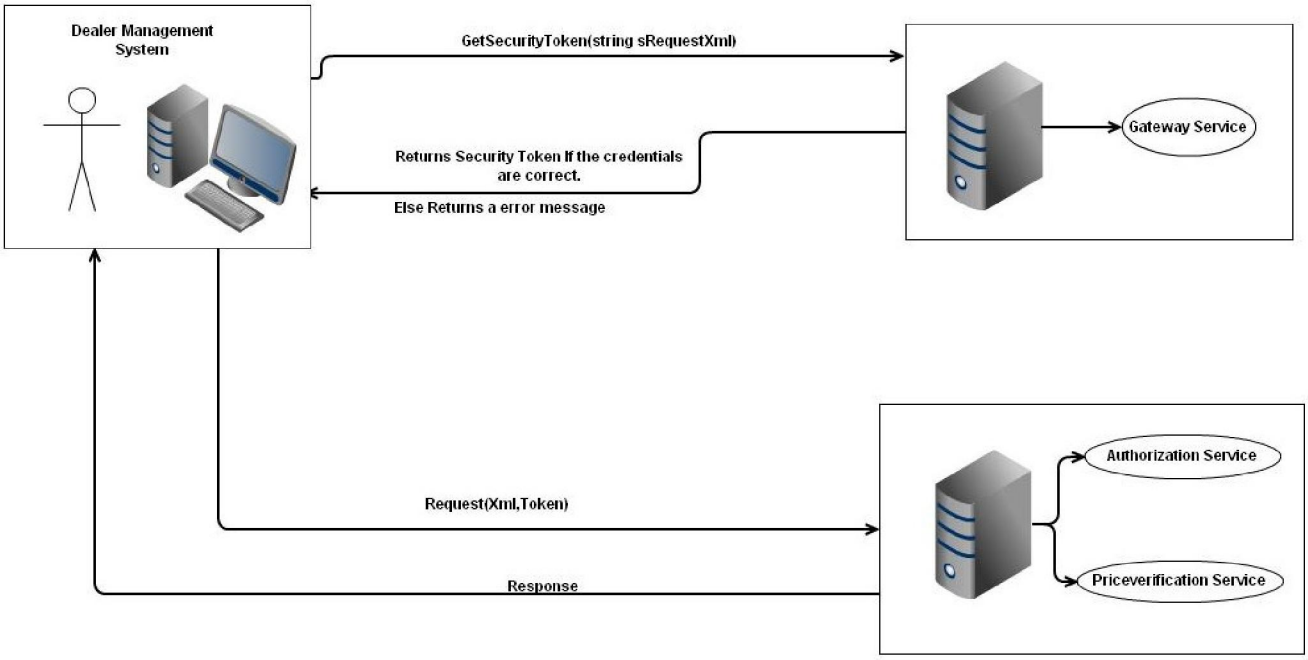
See the attached XML Schemas for formatting of the data (Strings, Monetary data, dates and others). **NOTE:** All of the XML tags will be required; however, certain tags are optional and can be empty. That is, if no data is present, then provide the tags with no data (I.E. <VIN></VIN>). See the following tables for more details on the optional tags.

4.1 URL address for the Gateway Service

Production URL:
https://csa.mvpreferred.com/GatewayService/Gatewayservice.asmx

User Acceptance Testing URL:
https://csauat.mvpreferred.com/GatewayService/Gatewayservice.asmx

4.2 Gateway Service Flowchart



4.3 Gateway Service Security Level

The DMS can call the Get Security Token method using one of three separate security levels. The security level for the DMS is checked and then validation and authentication is done for the request. Three security levels are explained below:

4.3.1 Security Level 1

Security Level 1 is authentication based on the IP address. It can be one single IP address or a range of IP addresses. The IP address of the request is checked against the IP address in the database for the DMS. If the IP address matches, then the token is returned with token life.

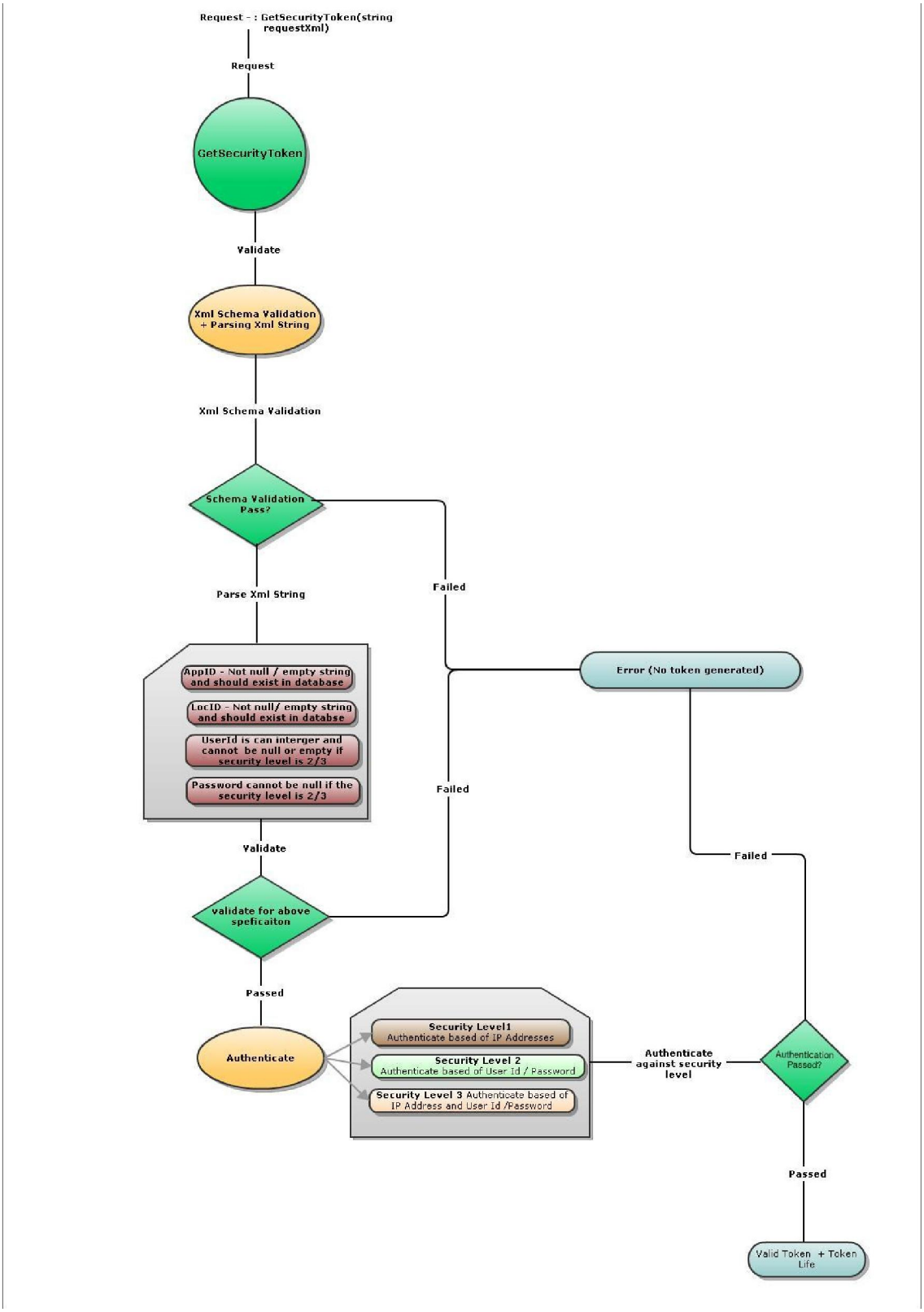
4.3.2 Security Level 2

Security Level 2 is authenticated based on the username and password. The request is validated against the username and password in the database for the DMS. If the username and password matches, then the token is returned with token life.

4.3.3 Security Level 3

Security Level 3 is a combination of Security Level 1 and Security Level 2. The request is validated against the IP Address(es) and Username/Password in the database for the DMS. If the information matches, then the token is returned with token life.

4.3.4 Security Level Flowchart



4.4 XML Get Security Token Request (DMS to MVPreferred)

Tag Identifier	Description / See XML Schema for formatting	Optional
TokenRequest	Beginning of Message Request	
AppID	Integer. Cannot be NULL or empty string. App ID assigned to the DMS	
LocID	Loc_ID cannot be NULL or empty string. Populate with Dealer Code.	
User_ID	If the security level is 2 or 3, then User_ID is an integer and cannot be NULL or empty string. If security level is not 2 or 3, then User_ID can be NULL or empty string.	Conditional
Password	If the security level is 2 or 3, then the Password cannot be NULL or empty string. If security level is not 2 or 3, then the Password can be NULL or empty string	Conditional
/TokenRequest	End of Message Request	

4.5 XML Get Security Token Response (MVPreferred to DMS)

Tag Identifier	Description / See XML Schema for formatting	Optional
TokenResponse	Beginning of Message Request	
Token	Unique GUID	
Token Life	Number of minutes before token expires	
RetCode	Return Status *See Return Status Code list*	
RetMsg	English error message to be Prompted onto DMS screen *See Return Status Codes list*	
/TokenResponse	End of Message Request	

4.6 Get Security Token Request - Samples

4.6.1 Get Security Token Request Sample XML

```
<?xml version="1.0" encoding="utf-8"?>
<tr:TokenRequest xmlns:tr="http://Volvo.Com/GetSecurityTokenRequest.xsd">
  <tr:AppID>99</tr:AppID>
  <tr:LocID>999K</tr:LocID>
  <tr:UserID>1234</tr:UserID>
  <tr:Password>test-1234</tr:Password>
</tr:TokenRequest>
```

4.6.2 Get Security Token Request XML Schema

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:tr="http://Volvo.Com/GetSecurityTokenRequest.xsd" attributeFormDefault="unqualified"
elementFormDefault="qualified" targetNamespace="http://Volvo.Com/GetSecurityTokenRequest.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="TokenRequest">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="AppID" type="xs:string" />
        <xs:element name="LocID" type="xs:string" />
        <xs:element name="UserID" type="xs:string" />
```

```
        <xs:element name="Password" type="xs:string" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

4.7 Get Security Token Response - Samples

4.7.1 Get Security Token Response XML

```
<?xml version="1.0" encoding="utf-8"?>
<tr:TokenResponse xmlns:tr="http://Volvo.Com/GetSecurityTokenResponse.xsd">
  <tr:Token>5464c3dd-2181-4d05-b496-cc88a3df9b2e</tr:Token>
  <tr:TokenLife>1440</tr:TokenLife>
  <tr:RetCode>1700</tr:RetCode>
  <tr:RetMsg>Success</tr:RetMsg>
</tr:TokenResponse>
```

4.7.2 Get Security Token Response XML Schema

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" targetNamespace="http://Volvo.Com/GetSecurityTokenResponse.xsd"
xmlns:mstns="http://Volvo.Com/GetSecurityTokenResponse.xsd"
xmlns="http://Volvo.Com/GetSecurityTokenResponse.xsd" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata" attributeFormDefault="qualified"
elementFormDefault="qualified">
  <xs:element name="TokenResponse" msdata:Prefix="tr">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Token" msdata:Prefix="tr" type="xs:string" minOccurs="0" />
        <xs:element name="TokenLife" msdata:Prefix="tr" type="xs:string" minOccurs="0" />
        <xs:element name="RetCode" msdata:Prefix="tr" type="xs:string" minOccurs="0" />
        <xs:element name="RetMsg" msdata:Prefix="tr" type="xs:string" minOccurs="0" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true"
msdata:Prefix="tr">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="TokenResponse" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

5.0 Return Status Codes and Messages

Gateway Service Error Codes					
RETURN CODE (<RetCode>)	**RETURN MESSAGE (<RetMsg>)**	**GATEWAY SERVICE ERROR NUMBER**	**ORIGINAL MESSAGE**	**PROBABLE CAUSES**	**SOLUTIONS**
0	1700 Success	1700	1700 Success	1. Security token returned.	1. Security token returned.
1	500 System error.	500	500 Internal Server Error	1. Internal Error.	1. Please call MV Preferred Technical Support at 336-931-3820
1	1701 Application ID does not exist.	1701	1701 Application ID not found.	1. Application ID not found in NATS system.	1. Try again with a valid Application ID
1	1702 Invalid Application ID.	1702	1702 Application ID is invalid.	1. Application ID entered is invalid.	1. Try again with a valid Application ID
1	1702 Location ID does not exist.	1703	1703 Location ID not found.	1. Location ID not found in NATS system.	1. Try again with a valid Location ID
1	1704 Invalid Location ID.	1704	1704 Location ID is invalid.	1. Location ID entered is invalid.	1. Try again with a valid Location ID
1	1705 UserID is Invalid	1705	1705 UserID is Invalid	1. UserID is null or empty.	1. Try again with a valid User ID.
1	1706 Password is Invalid	1706	1706 Password is Invalid	1. Password is null or empty.	1. Try again with a valid password.
1	1707 Invalid UserID and Password	1707	1707 UserID and Password are Invalid	1. UserID & Password are null or empty.	1. Try again with a valid User ID and password.
1	1708 IP address is out of range.	1708	1708 IP address is out of range.	1. IP address out of range.	1.Verify current IP address has been submitted to MV Preferred systems
1	1709 Login credentials are incorrect.	1709	1709 Username or password is incorrect.	1. Incorrect username or password.	1. Please check for the correct login credentials and try again.

Gateway Service Error Codes					
RETURN CODE (<RetCode>)	**RETURN MESSAGE (<RetMsg>)**	**GATEWAY SERVICE ERROR NUMBER**	**ORIGINAL MESSAGE**	**PROBABLE CAUSES**	**SOLUTIONS**
1	1710 IP Address is not in range and login credentials are invalid	1710	1710 IP Address is out of range and login credentials are incorrect	1. IP address out of range and user credentials incorrect	1. Verify current IP address has been submitted to MV Preferred systems 2. Please check for the correct login credentials and try again.
1	1711 XML received was invalid	1711	XML received was invalid	XML is missing a mandatory schema tag element or syntax is incorrect making the structure of the message invalid	Verify the structure of the XML document that is being sent to MVPreferred systems

6.0 Service Level Agreement

Response time for messages MUST be less than 15 seconds. If no response is received by the sender, assume a timeout occurred, and take appropriate action by aborting the request, or retrying.

- VFS IT DMS/Dealer network: the bandwidth and/or availability of the DMS and/or dealers connection from their respective Internet Service Provider is not in scope for VFS IT support
    - VFS IT SLA support covers incoming/outgoing connections to the gateway service designated in the specification

7.0 Glossary

Term	Description
Authorization and Settlement	Process where DMS send message to MVPreferred to get authorization to reserve line of credit for purchases. Settlement is the process where all authorizations are sent to MVPreferred at the end of the day for payment (NATS sends payments directly to the Dealers).
DMS - Dealer Management System	Software system that allows truck dealers to manage customers and fleet trucks
FTP – File Transfer Protocol	File Transfer Protocol, the protocol used on the Internet for exchanging files.
Gateway Service	Security protocol using token/GUID validation with Price Verification and Authorization requests
GUI – Graphical User Interface	Screens formatted for ease of reading and data entry.
HTTP - HyperText Transfer Protocol	The protocol for moving hypertext files across the Internet. Requires a HTTP client program on one end (Browser), and an HTTP server program on the other end. HTTP is the most important protocol used in the World Wide Web. See http://www.w3.org/Protocols/ for full specifications.
Line of Credit	Credit limit as authorized by NATS. The LOC will be maintained within Volvo's A/R system
Invoices	A business document that contains the names and addresses of the buyer and the seller, the date and terms of the sale, a description of the goods, the price of the goods, and the mode of transportation used to ship the goods. The seller calls the invoice a sales invoice; the buyer calls it a purchase invoice.
Real Time	Access electronic information immediately on demand
Repair Orders	Much like a sales order invoice (SOI) except final payment amount is not known until the repair is close to completion. Repair Orders can be authorized to set aside an estimate as to the amount needed for the repair.

TCP/IP	A suite of protocols that defines the Internet. Originally designed for the UNIX operating system, TCP/IP software is now available for every major kind of computer operating system.
Part Number	The manufacturer's/maker's number that uniquely identifies the product/resource.
Pull	Terminology commonly used to indicate receiving a computer file.
Push	Terminology commonly used to indicate sending files from a computer to another computer.
SFTP (Secure File Transfer Protocol)	Part of the SSH protocol suite which uses FTP file transfer with encryption.
SSH (Secure Shell)	Network protocol which provides a secure file transfer session between two networked systems.
VPN – Virtual Private Network	Acronym for Virtual Private Network. A VPN is a way to provide remote access to an organization's network via the Internet. VPNs send data over the public Internet through secure "tunnels."
Volvo Preferred Pricing System (MVPreferred)	Volvo system which provides pre-negotiated customized discount on parts and services.
NATS – North American Transaction Services	Volvo entity issuing credit to corporations to allow truck purchase and maintenance
MVPreferred	New Volvo system to allow DMS to lookup preferred pricing for fleet clients
VOLVO – Volvo Trucks North America	Volvo Trucks North America entity setting parts/product pricing for various fleet clients.
WAN - Wide Area Network	A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks
XML – Extensible Markup Language	A plain text language designed for large-scale electronic publishing. See http://www.w3.org/XML/Core/#Publications for full specifications