

INTTRA eInvoice – World Class Technology

Executive Summary

As the leading ocean industry portal, INTTRA is designed and operated to deliver a neutral, secure, and reliable platform to perform critical business transactions between shipping partners. With INTTRA eInvoice, both carriers and their customers will gain access to robust functionality and automated processes for reviewing, disputing, approving, paying and reconciling payments to invoices. INTTRA eInvoice, developed exclusively for the ocean freight industry, is based on the proven technology of Deutsche Bank's eBills electronic invoice presentment and payment platform and is delivered as a Software as a Service (SaaS) to minimize the impact on clients' IT resources. INTTRA eInvoice, like all INTTRA's SaaS products, are hosted in a premium data center based on world-class industry standards and operated by a global team 24x7x365.



This overview will provide you with a high level understanding of:

- The SaaS technology architecture
- Security implementation and practices
- Information technology service continuity

The INTTRA eInvoice system architecture is based on a secure, industry standard, three tier architecture. A High Availability (HA) server environment, utilizing both local and geographic load balancing, is employed to assure 99.95% availability.

Web Presentation Services

The primary function of the Web Presentation Services (WPS) is to deliver web pages to the user. The WPS delivers HTML and any additional content that may include images, flash objects, PDFs, and dynamically generated information to the user's web browser. Security hardened iPlanet Enterprise Web Servers operating on a secure Sun Solaris Operating System are implemented in this tier to provide WPS. One security feature, to ensure secure transactions, is the use of Verisign as the issuer and authority for INTTRA eInvoice Secured Sockets Layer (SSL) certificates. Verisign is the recognized global leader offering the most secure 128 bit encryption available today and serves more than 1 million Web Presentment Servers worldwide.



Web Application Services

The primary function of Web Application Services (WAS) is to provide a framework for the application of business rules or logic to transactional data. The INTTRA eInvoice platform operates on iPlanet BillerXpert, iPlanet Process Manager and iPlanet Application Server technology. These three powerful processing engines combine to deliver robust functionality and automated processes for all facets of invoice processing. These application servers operate on secure Solaris Operating Systems developed by Sun Microsystems.

Database Services

Database Services (DS) for INTTRA eInvoice is provided by the Oracle Enterprise Edition Relational Database Management System (RDBMS). The database engine is the underlying software component that an RDBMS uses to create, retrieve, update and delete data from the database. Oracle databases provide leading performance, scalability, security and reliability for the world's most heavily transacted industries including financial services, health care and consumer retail.

Security

Security, by one definition, is a state or condition which is resistant to harm. Therefore, security as a form of protection, are systems and processes that provide or improve security as a condition. Security must be considered as an overall program and not a single event or project. With INTRA eInvoice, as with all INTRA products, security is a multi-layered solution that considers both cyber and physical security. INTRA and its INTRA eInvoice delivery partner Deutsche Bank, maintain a 24x7x365 operations center to ensure product and services availability. Additionally, Deutsche Bank operates a 24x7x365 Security Operations Centre (dbSOC) to detect and respond to any security threat. Security is tested and includes annual network vulnerability assessment, external vulnerability scanning (weekly), internal vulnerability scanning (weekly), wireless vulnerability assessment (annual), scanning for non-standard desktops (ad-hoc) and end-to-end security monitoring testing (annual).



Security - Cyber Layer 1 – Firewalls

Firewalls are deployed throughout the technology architecture to create “security zones.” The first zone is the External Demilitarized Zone (EDMZ) containing the WPS. The second zone is the Internal Demilitarized Zone (IDMZ) containing the WAS. The final zone is the Internal Network Zone (INZ). Each zone provides specific levels of security, balancing the need for business transaction processing and the need to thwart any cyber attack. All users of INTRA eInvoice will only create a session in the EDMZ with the WPS.

Security – Cyber Layer 2 – SSL

SSL provides the ability to transact business via the Internet, assuring each business transaction is encrypted and not traversing the open Internet in plain sight. As mentioned earlier, Verisign is the provider of SSL certificates which utilizes 128 bit encryption for all INTRA eInvoice sessions.

Security – Cyber Layer 3 – N/HIDS

Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) provide forensics as an additional layer of protection. NIDS devices are placed in security zones EDMZ and IDMZ to determine abnormalities in traffic patterns or previously identified abnormal patterns. Patterns are regularly updated to ensure the latest worldwide attacks are registered and available for detection. HIDS is a software based solution which enrolls each network device, server (both operating system and application) and protection devices (firewalls, NIDS, etc.) and regularly compares the current configuration with the approved configuration. If the comparison fails to be equal, security alerts are raised for the Security Operations Centre (dbSOC).

Security – Cyber Layer 4 – Encrypted File Transmission

Files (data) are transmitted between four key entities: Biller, Payer, INTRA and Deutsche Bank. Carriers/NVOCCs can choose one of two secure file transmission protocols to connect to INTRA eInvoice:

1. Secure File Transfer Protocol (SFTP)
2. EDI Over the Internet (EDIINT), specifically Applicability Statement 2 (AS2) for HTTPS protocol, synchronous – Peer-to-Peer, Real Time utilizing S/MIME encryption.

Both protocols utilize public key / private key exchanges to ensure security and data encryption. INTRA recommends the AS2 protocol because of its inherent confirmation of transmission receipt through the use of Message Disposition Notifications (MDNs). MDNs provide both positive and negative confirmation of file receipt and provide end-to-end traceability of all file transmissions.

Security – Physical Layer 1 – Surveillance Cameras

At the core of all SaaS providers is the data center. Put another way, it is the manufacturing and servicing plant of the finished products the SaaS provider sells to the market and, as one of the company's most important assets, requires protection. The first layer of protection is utilizing surveillance cameras with video recording. These cameras are positioned to capture activity at all entrances and exits to the data center. Additionally, the Deutsche Bank data centers are guarded 24x7x365 by external security agencies who vigilantly monitor the live security video.

Security – Physical Layer 2 – Ingress Access Security

Physical access to the data center is only granted to persons requiring the need to physically install, de-install, repair or otherwise maintain any asset within the data center. An employee, whose job responsibility requires this access, is typically granted access 24x7x365. All non-employees, who require physical access to the data center, are granted access on an exception basis and must be accompanied by an authorized employee at all times. Physical access to the data center is restricted by two factor identity authentication; a proximity access card security system and bio-metric access mechanisms or cipher lock. Two factor authentication assures identity and removes the possibility of access from a lost or stolen access card.

Information Technology Service Continuity

Information Technology Service Continuity (ITSC) is a set of policies, process and procedures that facilitate the recovery or continuance of critical business technology infrastructure after a natural or human induced disaster. ITSC begins early in the Business Solution Development Life Cycle (BSDLC) to ensure the solution's market viability and sustainability. The INTRA eInvoice Service Level Agreement (SLA) or Recovery Time Objective (RTO) is four hours from point of disaster declaration.

Highly Available Data Centers

The foundations for highly available data centers are the utilities which serve them.



Each data center is supplied electrical power from the prevailing public electric utility and on-site backup generators (when required). These power sources feed Uninterruptible Power Supply Systems (UPS) which serve two functions: they provide backup electrical power (via batteries) for a period of time which allows the transition from utility power to generator (and vice-versa), and stable and "clean" electricity to the computing plant.

Technology infrastructure produces a good deal of heat. Redundant Computer Room Air Conditioning (CRAC) units provide cold filtered air to all equipment within the data center. The final "utility" is fire detection and fire suppression. Each data center maintains a fire detection system and a non-liquid fire suppression system.

Geographically Diverse Data centers

The next layer of defense for a successful ITSC, is to have multiple data centers geographically apart to avoid a reasonably widespread disaster affecting the recovery / continuance of the business. The INTRA eInvoice system architecture utilizes this capability to ensure timely recovery and business continuance. Additionally, Deutsche Bank's INTRA eInvoice DS tier is securely replicated to a "sister" data center, in real-time, ensuring minimal to no data loss in the event of fail-over. Deutsche Bank's WPS and WAS tiers are configured as active-active with geographic load balancing between data centers. This provides two benefits; continuously operational recovery systems and minimized recovery time to connect to the DS tier.

Off-Site Data Retention

Data protection is paramount to providing the INTRA eInvoice solution. The Deutsche Bank DS tier is protected by an enterprise class tape backup system. The INTRA eInvoice database and file systems are backed up weekly (retained for 7 years) and monthly (retained for 1 year) and are stored at a secure off-site facility as per regulatory requirements.

About INTRA

The Largest Multi-Carrier E-Commerce Platform for Global Shipping

INTRA is a leading global provider of e-commerce solutions to the ocean freight industry. INTRA professionals work with over 30 leading carriers and their customers to streamline and standardize their shipping processes worldwide through a network of more than 20,000 corporate locations. Over 350,000 container orders are initiated on the INTRA platform each week, representing more than 12 percent of global ocean container trade.

INTRA Corporate Headquarters

Morris Corporate Center II
One Upper Pond Road
Building D
Parsippany, NJ 07054
USA

Tel: +1.973.263.5100

Fax: +1.973.263.5969

