

securityPAQ™ by TRADEPAQ

Enhanced Security for Your Shipping Documents



Overview

TRADEPAQ Corporation provides a comprehensive solution for secure physical printing using the TRADEPAQ for Exchanges, Banks, Logistics and Enterprises™ product suite.

Today's times require new measures be put in place to secure international shipments. Forwarders are making significant investments to screen, inspect, and verify the contents of shipments to enable secure containerization. Exporters are enhancing physical security measures at shipping docks. Carriers are requiring authorized inspections and security certifications before accepting cargo for transport. Importers that have had to deal with shrinkage and fraud, now have to verify security as well.

Until now, secure document authentication was something required for shipments using Letters of Credit payment. An original authentic bill of lading, commercial invoice, packing list and certificate of origin verified by the parties in a trade were required to ship the goods and get paid. But with Letters of Credit accounting for only a portion of international transactions, the same strict attention to detail PLUS additional security measures that establish authenticity have to be applied to all international as well as many domestic shipments.

TRADEPAQ has been offering document solutions for Letter of Credit transactions for a decade. Today, TRADEPAQ provides secure international and domestic documentation systems tailored specifically for the needs of your trade chain. By adding SecurityPAQ to any TRADEPAQ document solution, you can ship the goods safely, get paid faster, and measurably reduce supply chain execution costs.

SecurityPAQ™ Functions

- **Tamper-Proof Electronic Documents:** Documents images and XMLs are delivered electronically via the Internet through secure means that eliminate the opportunity for tampering with the data.
- **Authentication of each user:** Data sources and users are authenticated using passwords, smart cards, and/or other high security methods. Optional fingerprint identification and even retinal scanning are available for ultra-high security environments.
- **Restricted Printing w/Limited number of secure copies:** Print only the number of authorized originals and copies at the designated print location.

Receive confirmation where, when, and how many documents were printed. Special papers and inks may be used to eliminate the possibility of unauthorized copies.

- **Non-repudiable transactions:** Receive verifications indicating that documents were received by the intended parties. No more excuses that the documents were not received, plus they can't get lost!
- **Verifiable Output w/Secure Archive:** The output is verified via audit trails and archives. Documents can be checked against the source image through the internet. Authorized parties can view archived images of documents, with reprint, fax, and e-mail available.
- **Roles Based Internet Access:** Complete roles based security enables the right people to access their authorized set of documents and functions.

Technical Overview

1. SD Express Printing Solution

The SD Express utilizes data encryption to protect documents from unauthorized access and alterations. The encryption used is the Rijndael encryption algorithm. Rijndael is the new advanced Encryption Standard (AES) of the National Institute of Science and Technology.

The SD Express solution waits until the moment of printing to decrypt the printer-bound data, protecting the document throughout the entire transmission process. In the event that the document is somehow routed to the wrong location, encryption makes the resulting output unreadable. Remote users can print to SD Express-equipped printers from anywhere on the web. Data encryption ensures privacy and document integrity throughout the web transmission process.

To deliver these capabilities the SD Express solution leverages HP Chai Server technology, which gives HP Laserjet printers the ability to connect directly to the web using standard web protocols such as HTTP and MIME. To print a secure document remotely, the TRADEPAQ document solution routes the documents in the same manner as a regular network printer. The SD Express software automatically encrypts the data and emails it to the SD Express-equipped HP Laserjet Printer without further user intervention. Once the file is received, the printer emails an acknowledgment of receipt to the sender and decrypts the document just prior to printing.

2. Embedded Java secure Printing Solution Option

The Embedded Java secure Printing Solution utilizes an embedded Java program in the remote printer to manage the print job. The solution requires the following environment. HP Laserjet printers of the type 4100, 4550 or 9000, equipped with:

- Duplex option
- Embedded web server
- Harddisk
- Network Interface Card with SMTP support for example HP Jet direct 610
- Support for the Laserjet Chai Development platform

The Embedded Java secure Printing Solution is based on the mechanism of working with fixed IP-addresses to determine the correct printer. The TRADEPAQ document solution transmits the file (not the print job) encrypted to the Embedded Java program in the printer. The file is captured and decrypted by the Embedded Java program where after the program will create and manage the print job. The Embedded Java program will confirm the status of the print job to the remote user. The program is also capable of disabling features like hardware copies on the printer itself.

3. Authentication, Encryption, and Authorization options

SecurityPAQ™ SafeGuard® PKI for producing digital certificates. SafeGuard® PKI is the enabling technology needed for the generation, verification and management of certificates. It provides a secure platform and Public Key Infrastructure (PKI) for Public Key-enabled Applications (PKAs). Such applications allow, for example, secure interchange of data and strong user authentication. Due to its flexibility and scalability, SafeGuard® PKI can easily be adapted to a wide range of security policies.

SecurityPAQ™ SafeGuard® Toolkit. The SafeGuard® Toolkit is an ANSI-C library, which provides all necessary cryptographic and administrative functions to build secure electronic messaging systems, EDI systems, Telebanking applications, Electronic Commerce systems and Public Key Infrastructure components in an easy way. SafeGuard® Toolkit has an open architecture. Fast software implementations of commercial algorithms, such as RSA, AES, triple-DES, IDEA, SQUARE, RIPEMD160, MD5, SHA-1 are available. Furthermore, protocols and standards such as X.509v3, S/MIMEv2 and v3.1,

PKCS#7, MailTrusTv1.1, PKCS#11, etc. are also supported. The toolkit is also designed to accommodate alternatives (e.g. PEM, PKIX, etc.) and various off-the-shelf hardware options. SafeGuard® Toolkit is multi-platform. By default it supports the Windows 32 bit platforms. In addition, it is already ported to many platforms, e.g. OS/2, many UNIX versions, and can be ported to other platforms on request.

SecurityPAQ™ HSM for storage of Root CA keys and time stamping payment transactions. The CryptoServer® 2000 Hardware Security Module (HSM) has been developed for use in applications and environments that require a very high standard of security. In addition to an above-average level of physical security, high performance is often also required in this context. Thanks to its ingenious physical tamper-protection system, the CryptoServer® 2000 module reacts autonomously to attempts at tampering and ensures the integrity and confidentiality of the key information. Furthermore, the CryptoServer® 2000 module also offers the highest level of security when it comes to generating, storing, archiving, cloning, migrating and managing keys. Certification according to Common Criteria EAL4 high and ZKA is in progress. The design is also already prepared for certification according to FIPS140-1 level 4.

SecurityPAQ™ SafeGuard® Transaction Client. SafeGuard® Transaction Client is a browser plug-in for digitally signing web-based transactions. It is seamlessly integrated into both Microsoft Internet Explorer and Netscape Communicator and also comes with a Java API. The Java API gives applets easy access to sophisticated features like smartcard's and WYSIWYS (What You See Is What You Sign). SafeGuard® Transaction Client offers you and your customers a simple way of signing any web-based content or transaction.

SecurityPAQ™ SafeGuard® Sign & Crypt for Adobe Acrobat. SafeGuard® Sign & Crypt for Adobe Acrobat is available in three versions:

- As signature plug-in for Adobe Acrobat (the full version, not the Acrobat Reader) for corporate use.
- Also available as a stand-alone utility to sign and verify PDF files (no Adobe Acrobat needed) for corporate use.
- Or as a stand-alone utility to verify PDF files (no Adobe Acrobat needed) for unlimited distribution to a company's customer circle.

All these products are part of the SafeGuard® Sign&Crypt range and are a first set of solutions for digital signatures in document management and workflow environments.

SafeGuard® is a registered trademark of Utimaco Safeware.

Utimaco Safeware offers a comprehensive product portfolio to meet all requirements for secure infrastructures, based on PKI

(public key infrastructure), as well as PKI-enabled applications using, among others, smartcards and biometrics for authentication, electronic signatures and encryption. In 1997, the company was the first manufacturer to supply a signature solution that met legal requirements, and is seen internationally as one of the pioneers and leading suppliers in this area. It is the worldwide market leader in the provision of electronic signatures based on biometrics. Utimaco Safeware's PKI Technology was selected as Reference Implementation for the EU-financed "pki Challenge" initiative that include the leading international manufacturers of PKI solutions. Utimaco Safeware's PKI technology is used for the National PKI in Bulgaria, by CSSF (organization for banks in Luxembourg), CertEurope (TTP in France), DBV-Winterthur (Switzerland), the FöreningsSparbanken AB (Sweden), the Ministry of Justice of the state of Baden-Württemberg (Germany), the Ministry of Justice, the Netherlands and many others.

SecurityPAQ™ smartcard readers or biometrical smartcard readers

- The CardMan® reader allows secure use of home banking, e-commerce, digital signatures, Single Sign On, cash cards, e-mails and certificate-based authorization. CardMan® readers are also compliant with the German Digital Signature Act (including legally binding web based transactions). All CardMan® products correspond to the ISO 7816 standard.

- Or choose the convenient fingerprint-based logon device from Precise Biometrics™, features fingerprint verification through Precise Biometrics' unique image processing algorithm in real time for highest security (patent pending). The fingerprint reader brings fingerprint logon to your desktop. The system supports both local MS Windows workstation logon and domain logon controlled by an MS Windows domain server.

4. Secure Transmission and Non-repudiation using bolero.net™

TRADEPAQ document solutions and boleroPAQ™ provide:

- Authentication - digital certificate-based security authenticates trade chain member identities.
- Certainty - affirmation and confirmation of transactions via bolero.net. Digitally signed title documents can be sent and/or confirmed to provide legal and non-repudiable proof of the transaction. Buyers and sellers complete the purchase process by securely exchanging contracts.
- Trust - the Bolero Rule Book gives exchanges the legal standards required in the international trade environment.
- Automation - electronic documents utilize bolero.net's validated XML DTD standards solution that allows the trade chain to seamlessly share data by automating their information exchange standards and processes.

How does this work?

- Pre-requisite: One of TRADEPAQ's document solutions is required. Choose TRADEPAQ for Logistics, Banks, Exchanges, or Enterprises that best fits your organization.
- Site survey: Security measures are determined based upon trade chain, organization, and product requirements. A TRADEPAQ team of security experts will spend a few days to determine your exact operational requirements.
- Integration: TRADEPAQ provides software and implementation services. We integrate third party devices and infrastructures from leading manufacturers with our document and security infrastructure.
- Deployment: The human element of security requires training for site specific security methods. TRADEPAQ's expert team provides training and deployment of systems.
- On going support: TRADEPAQ offers security infrastructure updates to match the client's needs with a program designed to maintain secure documents as technology changes occur.



All TRADEPAQ products and services referenced herein are registered trademarks or trademarks of TRADEPAQ Corporation. All other products and company names are trademarks of their respective companies.

© 1999-2002 TRADEPAQ Corporation

World Headquarters

TRADEPAQ Corporation
33 Maiden Lane
New York, NY 10038
USA
Tel: 212-482-8080
Fax: 212-482-8081
info@tradepaq.com

European Headquarters

TRADEPAQ Corporation
Tolweg 2
3851 SK Ermelo
The Netherlands
Tel: +31 341-556 166
Fax: +31 341-554 332
info@tradepaq.com

<http://www.tradepaq.com>

All Rights reserved. Printed in The Netherlands