Version 1.0

03 October 2003

SLIFT Pro version 1.0s – A Secure and Lightweight File Transfer Solution

Introduction

Organizations today rely heavily on Internet-based file transfer and data exchange as a basis of communications. The Internet provides a fast and efficient way to transfer files, effectively reducing overhead cost by obliterating the need to rely on manual shipping or courier services. Many a times mission critical files are being transferred in open network over the internet without taking into consideration factors like security, file authenticity and file integrity.

SLIFT Pro v1.0s, the latest addition in the SLIFT suite of products is a Client-Server Secure File Transfer solution for B2B operations. Together, it address the files transfer security problems stated above by providing user-friendly secure file exchange capabilities built on Public Key Infrastructure (PKI).

With strong cryptographic and verification capabilities as conforming to the PKI, SLIFT Pro v1.0s gives assurance of data confidentiality, integrity and non-repudiation of document delivery receipt. Supporting both manual and auto scheduling files transfer, files will be encrypted right before a file transfer is initiated and the files will never be decrypted until it reaches its intended recipient. The files transportation layer is also protected by Secure Socket Layer (SSL), further enhancing the end-to-end security of SLIFT Pro's architecture.

Purpose

This paper provides an overview of SLIFT Pro v1.0s, illustrating its architectural design, its business and security benefits, and its application deployment scenarios.

Other security solutions provided by PrivyLink include other SLIFT suite of products (SLIFT-Ez, SLIFT Classic), Cryptographic Key Server, Internet Application Security Solutions – both PKI and PIN based, TrustField Platform SDK and Virtual Token Server. Details of these solutions are described in the respective white papers for these solutions.

Architectural Design

Components

The SLIFT Pro is a sophisticated client-server software, with 2 variations of clients. It can be either an automated transfer client (SLIFT Pro AT) or an interactive one (SLIFT Pro iClient).

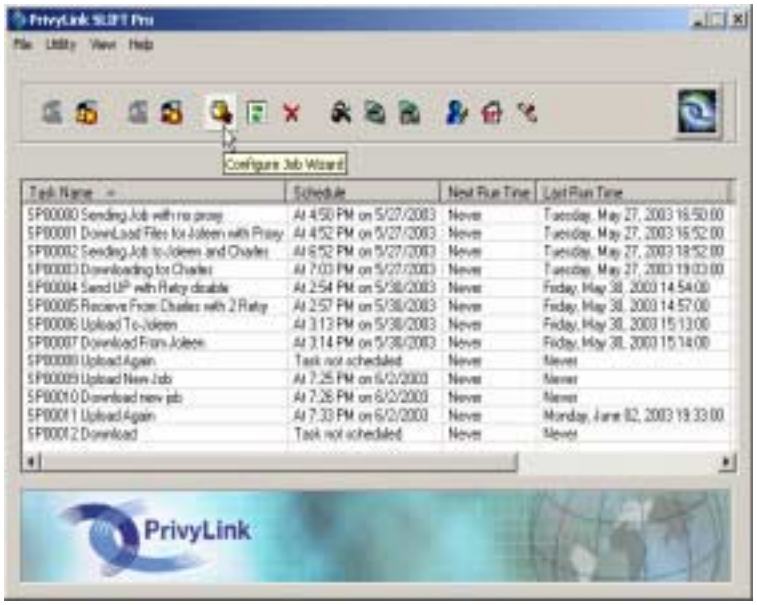


Figure 1.0 – SLIFT Pro Client Auto-Transfer (SLIFT Pro AT) Main GUI

Figure 1.1 – SLIFT Pro Client Interactive (SLIFT Pro-I) Main GUI

The SLIFT Pro Client has the capabilities to schedule file transfer jobs with the user friendly AT client, at the same time supporting manual file transfer using the SLIFT Pro iClient. By making use of the TrustField Platform, the SLIFT Pro clients also encompasses sender and recipient keys/certificates, and some verification modules that greatly facilitate secure file exchange between multiple parties (Files are exchange using FTP-SSL).

SLIFT Pro Client also contains a few levels of password management, namely the system password, application password (operator), user private key protection password and SLIFT Pro server account password. A combination of all these passwords will greatly increase the security and user feasibility of the whole system from a user's point of view.

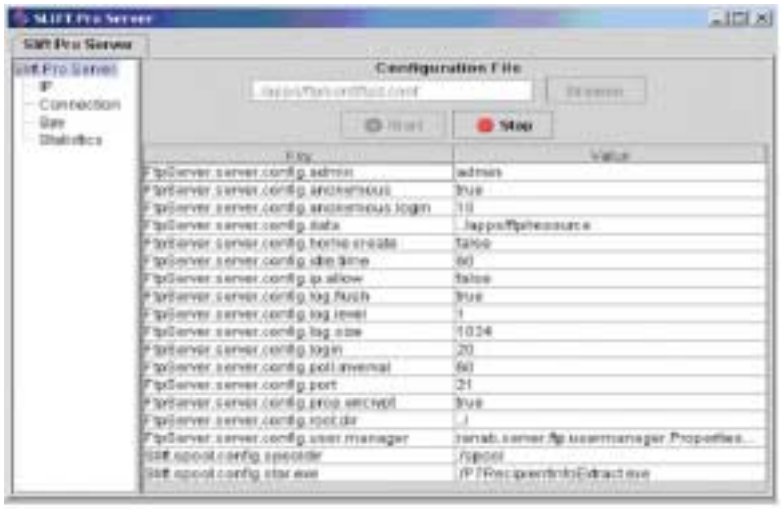


Figure 2.0 – SLIFT Pro Server Main GUI

SLIFT Pro Server is a backend server that acts as a secure file exchange centre for multiple SLIFT Pro Clients. Files will always stay encrypted in the SLIFT Pro Server in PKCS#7 formats, doubling the functionality of the server as a secure file repository.

It also bundles together an administration program, in which the encrypted files in the SLIFT Pro Server can be directly administered by the server itself.

Secure Files Exchange Protocol

The underlying transmission protocol for SLIFT Pro will be using File Transfer Protocol (FTP), in order to facilitate interoperability. FTP has been the default file exchange protocol for many organizations since many years, thus making SLIFT Pro extremely versatile in its deployment to many types of environment. By supporting both *active* and *passive* FTP protocol, SLIFT Pro is firewall/proxy-friendly and is able to be deployed to environment that calls for the strictest security protection.

File Security Protocol

SLIFT Pro is making use of Public Key Cryptographic Standards (PKCS), ITU-X.509 and RSA for its end-to-end file security cryptographic operations. The strength of the encryption is up to 168 bits for symmetric key operations and 2048 bits for public key operations.

Together with digital signatures technology, SLIFT Pro is able to provide file authenticity, file integrity and the underlying PKCS cryptographic operation to the file will provide confidentiality to the user.

Channel Security Protocol

To further strengthen the security, SLIFT Pro can be configured to support SSL (later known as TLS) as another layer of protection.

Benefits

- Sending/receiving of documents over the internet, extranet and intranet securely and efficiently.
- Protection of Files – Confidentiality, Non-Repudiation, Integrity and Authenticity.
- End-to-end security – files not decrypted until it reaches the intended recipient.
- Key Management by using certificates and private keys.
- File Management at the server based on file size, file date and file owner.
- Delivery management based on sender, recipient and X.509 certificates
- Supports multiple signatures on the same document to align with business workflow and approval processes
- Use of digital certificates issued by both Enterprise Certification Authorities (CAs) and publicly recognized CAs. The communicating parties need not use the same CA for protection needed.
- International standards compliance for both cryptography and file transport mechanism.

International Security Compliance

PKCS#1, #5, #7, #8, #11, #12

RSA 2048-bit Encryption and Digital Signature

US NIST FIPS-46-3 Triple-DES/DES Cryptographic Algorithm

US NIST FIPS-180-1 Secure Hash Function (SHA-1) Message Digest Algorithm

System Requirements

SLIFT Pro Client

Operating System: Windows™ NT/2000/XP (Windows is a trademark of Microsoft Corporation)

Memory: Minimum 64 MB RAM and 15 MB hard disk space

SLIFT Pro Server

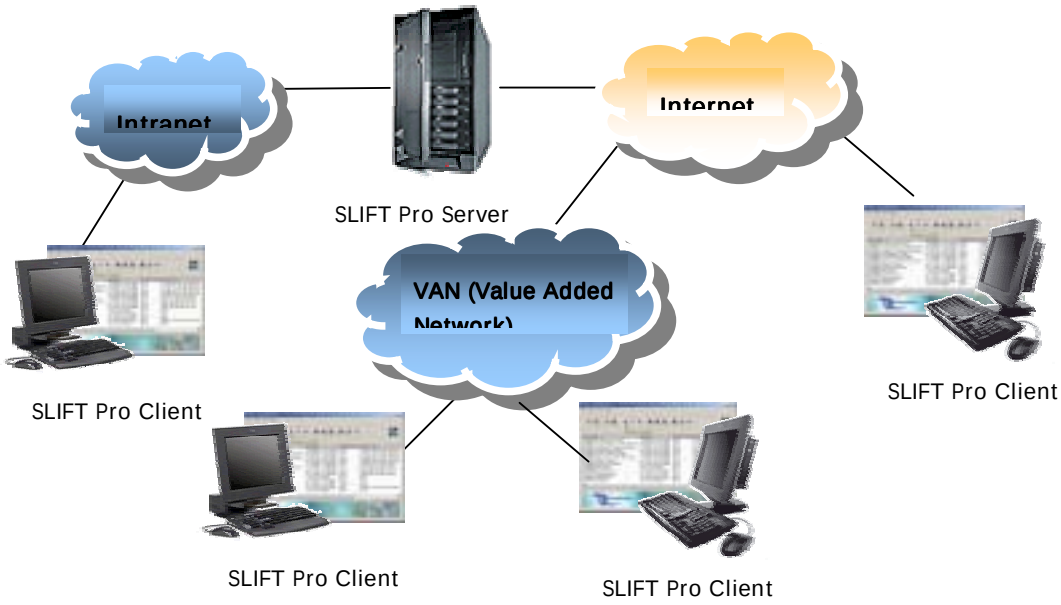
JRE 1.41 installed

JDBC compliant database installed

Operating System: Any platform which supports JRE version 1.4.1

Memory: Minimum 128 MB, hard disk as large as possible to store files, minimum 20 MB to store server application only

Deployment Architecture



About Privylink

Founded in 1997, PrivyLink is a response to strong industrial demands for high assurance delivery channel for electronic transactions, especially in the government and financial sectors. PrivyLink offers a comprehensive suite of software and hardware solutions to address end-to-end e-Security of today and tomorrow's businesses in the e-Commerce, e-Business, and e-Marketplace arenas.