International Financial System

Security Handbook

Last updated: 04 April 2022

Contact

Postal Technology Centre - Universal Postal Union Weltpoststrasse 4, 3015 Bern - Switzerland

Phone: +41 31 350 31 11

Service Desk Portal: https://support.upu.int

This document and the associated software contain proprietary information of the Universal Postal Union (UPU) and are provided under a specific agreement with eligible postal entities stipulating restrictions on use and disclosure. This document and the associated software are protected by law, including, as applicable, copyright laws.

This document and the associated software may not be, partly or as a whole, copied, disassembled, decompiled, modified or reverse-engineered without the express written permission from the UPU.

References in this publication to UPU products, applications, or services do not imply that the UPU intends to, or can make the said software, products, applications, or services, or parts thereof, available in all UPU member countries. Furthermore, no reference to a UPU software, product, application, or service is intended to state or imply that only UPU software, products, applications, or services may be used. Evaluation and verification of operation in conjunction with other products, applications, or services, except those expressly designated by the UPU, are the responsibility of the user.

Any references to particular designations of countries or territories shall not imply any endorsement or judgement by the UPU as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries. Moreover, any references to names of specific companies or products (whether or not indicated as registered) shall not imply any intention to infringe proprietary rights, nor shall it be construed as an endorsement or recommendation on the part of the UPU.

The UPU shall not be liable for any loss or damage arising from, or directly or indirectly connected to, the use of, reference to, or reliance on the associated software or any other UPU product, application, or service, including, but not limited to, any liability arising from negligent misuse, errors, disclosure, undue transfer, loss or destruction of data that may occur.

Any trademarks mentioned or referred to in this document and the associated software are the property of their respective owners.

The information in this document, including uniform resource locators (URLs) and other website references, is subject to change without notice.

Nothing in or relating to this notice shall be deemed or interpreted as a waiver, express or implied, of the privileges and immunities enjoyed by the UPU as an intergovernmental organization and specialized agency of the United Nations.

PTC
PostalTechnologyCentre
UNIVERSAL POSTAL UNION

Table of contents

About this guide

Intended audience

This guide is intended for use by IFS Network System Administrators and members of the PTC of the UPU who are responsible for ensuring security in the installation and implementation of IFS network systems.

How to use this manual

This handbook provides practical guidance on how to secure IFS information and services. For information on:

- the security that is inherent in IFS, see "Built-in Security in IFS" on page 8
- the security measures that each organization must put in place, "Security in the Customer’s infrastructure" on page 13
- resources for additional information, see "Where to go for more information" on page 24

You may not copy, rewrite or redistribute this document in any form. To do so is a violation of international copyright laws. However, the Postal Technology Centre welcomes your input. For queries or service requests, you can raise them at https://support.upu.int.

IFS and data security

IFS is an application that automates the processing and management of international and domestic money orders. IFS exchanges international money order data between sending and receiving organizations using Electronic Data Interchange (EDI).

Because processing money orders involves the electronic transfer of large amounts of financial data, effective security is vital. The IFS application uses a combination of technologies to ensure that money order data is transported and stored safely.

In addition, certain security measures must be in place within each customer's operating environment to protect against unauthorized access. This document explains the security measures that are inherent in IFS and provides basic information about the recommended security measures that you must implement within your organization's IFS environment to secure your data.

Two types of security

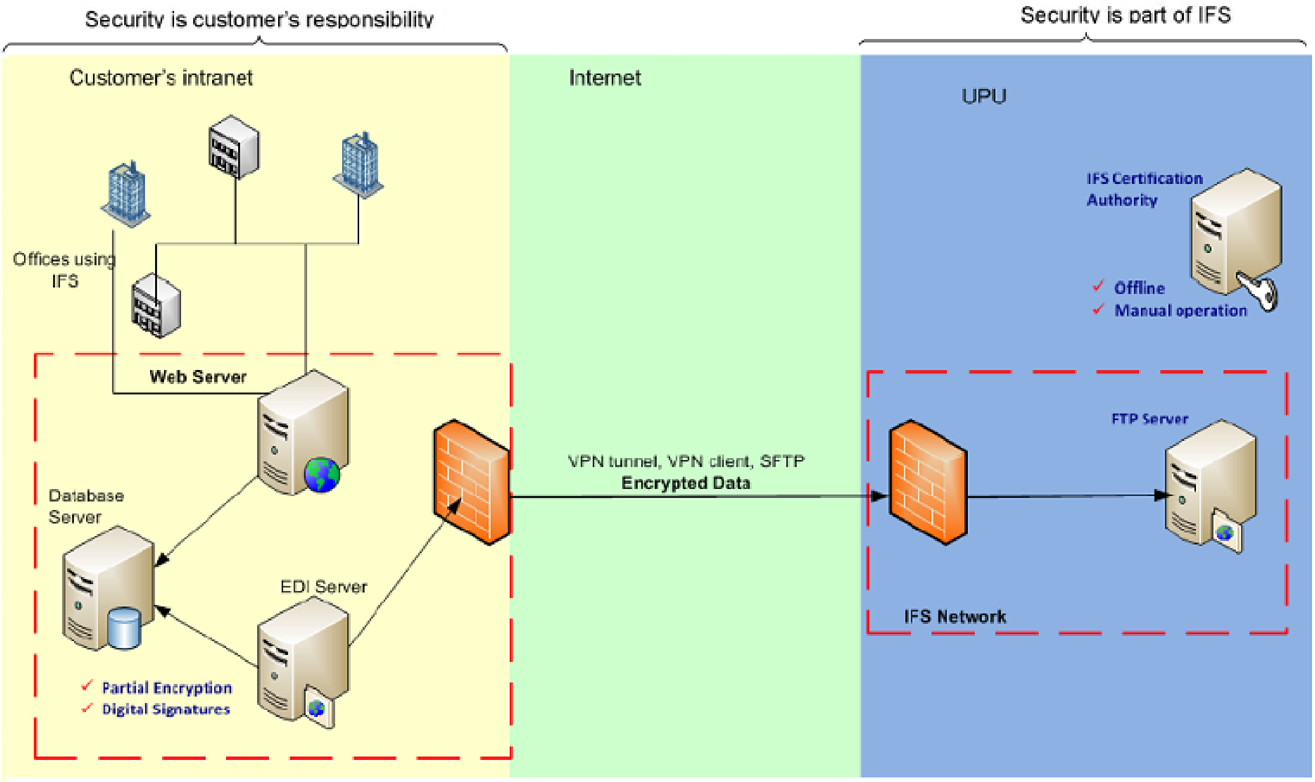
In every IFS installation, there are two important security aspects to consider. One is the security that is inherent in IFS. This encompasses the security that is part of the IFS application and network and is included in all IFS installations. The second aspect is the security measures that must be in place within each customer's organization. Each IFS customer is responsible for this aspect of security.

Overview of the IFS infrastructure

Money orders are created at a customer site using the IFS application. The components of this application are installed on one or more servers in the customer's intranet. IFS users access the application functions from a browser window. Transaction data is stored in a database. The international money order data is encrypted, digitally signed and transmitted over the IFS network. Domestic money order data is not required to be transmitted outside the customer's intranet.

At each customer site, the IFS system is installed within the customer's company intranet and consists of three main components:

- Web server – the machine on which the IFS application is installed
- Database server – the machine that hosts the IFS database
- EDI server – the machine that partially encrypts the international money order messages and sends them to the UPU



In the above diagram, it is important to understand that the components are conceptual and not necessarily separate physical pieces of hardware. In practice, the web server, database server, and EDI server components may be installed on separate machines, or one machine may serve as two kinds of server. For example, one machine may function as the web server and database server. However, it is equally possible to use three separate machines. The PTC supports a limited number of configurations. These configurations are explained in detail in the document *IFS Installation Guide*. For security reasons, it is not recommended to use the same machine as both an EDI server and Web server because of the increased vulnerability of unauthorized access to the EDI data from the Web.

General security goals

IFS accommodates many types of organizational structures, so there is not one particular configuration requirement that applies to every installation. Each IFS customer is responsible for determining the best configuration to use in terms of network security. Any security plan must address the following basic security objectives:

- *Confidentiality*: ensure that information is available only to those with authorized access. Confidentiality protects the privacy of information being exchanged between communicating parties. A VPN (Virtual Private Network/SFTP) connection and message encryption is used to ensure confidentiality of IFS data.
- *Integrity*: assurance that data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed. Digital signatures are used in IFS to protect integrity at the message level. Data integrity can be broken down into sub-elements:

  - Authentication: assurance that data comes from the source that claims to be sending it
  - Non-repudiation: assurance that the sender cannot deny having sent data and the recipient cannot deny having received it
  - Accountability: the system can identify the actions and behavior of a single individual within the system

- *Availability*: assurance that a system, service or data can be accessed and is protected against accidental or malicious destruction or denial of service attacks. A VPN/SFTP connection is used to protect the FTP server from attacks that could compromise the availability of the network.

Aspects of security

In order to meet the aforementioned goals, it is necessary to take a holistic approach to security and consider its different aspects beyond technological security:

- Physical security: this aspect refers to limiting access to a physical space. For instance, only certain employees (e.g. system administrators) should have access to the server room where the IFS database server is installed. Physical security also refers to preventing document theft and information leakage. If a paper process is involved (e.g. money orders issued in remotely located post-offices), documents should be duly archived in a secured area, and shredded when disposed of.
- Technological security: at the application level, multiple mechanisms have been built into IFS to ensure a high security standard. At the infrastructure level (i.e. browsers, OS, network), postal operators are responsible for providing a secured IT environment.
- Policies and procedures: should serve as educational guidelines to make employees aware of the importance of each individual's role in security. Employees should be trained to be vigilant when using IFS and be aware of any attempts at fraud and deception.

Built-in Security in IFS

The IFS FTP Server

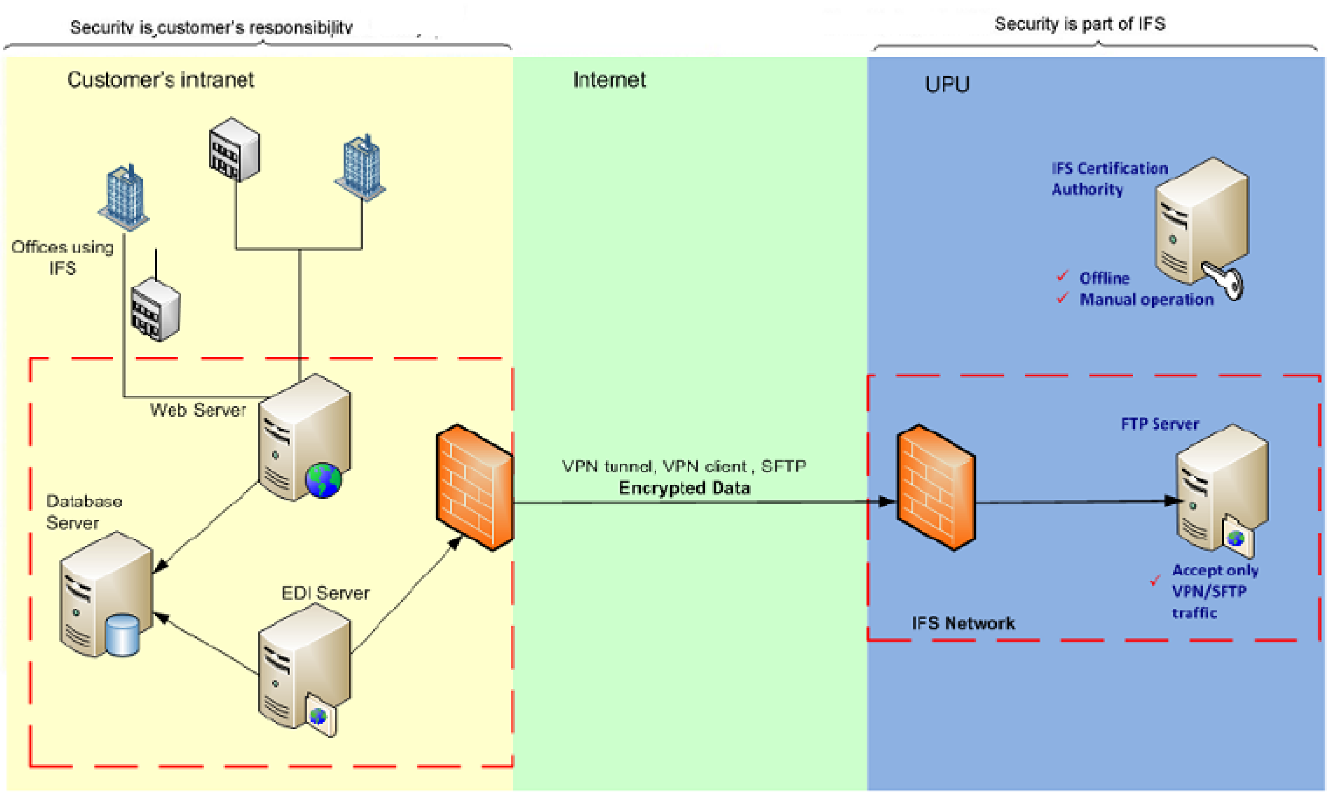
Encrypted money order data is exchanged between countries over the IFS network. The main component of the IFS network is the FTP server. Each member organization has its own directory on this server. The directories are structured by product and product type. The FTP server does not send data. The FTP server works by accepting money order traffic from IFS customers and posting the messages in the appropriate directory of the partner country.

The public certificates are also published on this server, and new encryption and signing requests as well as revocation alerts are posted on this server. Access to the FTP directory from the Internet is protected by a firewall for security, and the FTP server accepts only VPN traffic and SFTP connection. Every user, in this case an organization using IFS, authenticates on the FTP server to access its directory. An organization cannot access any directory on the FTP server other than its own.

Digital certificates

The certificate server at the UPU is the machine that hosts the Certification Authority (CA) software that specifically handles IFS encryption and signing certificates. The certificate server contains the private key and is the only machine to have access to this key. To prevent any possibility of unauthorized access, the certificate server is a stand-alone machine that is not physically connected to any network. Information is transferred from the CA server to the FTP server off-line.

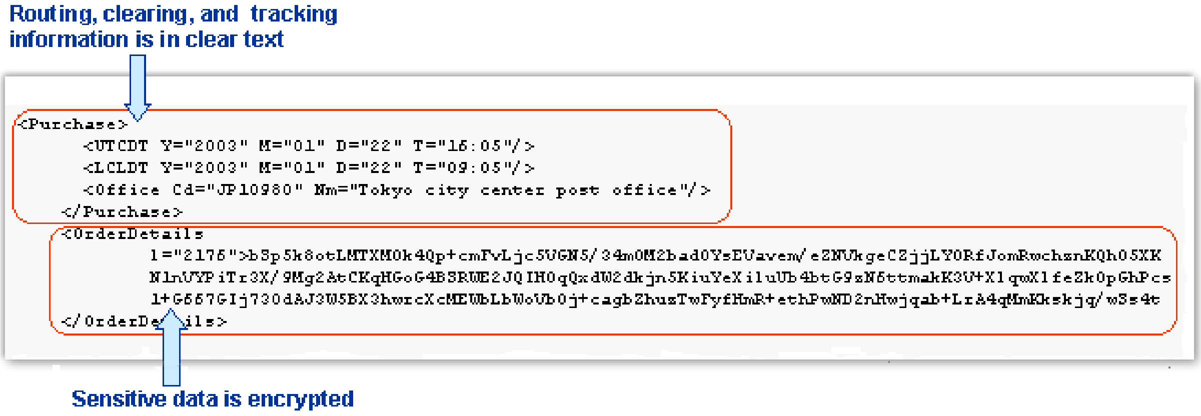
IFS uses two kinds of electronic certificates to ensure data safety and integrity. A license certificate is the license that allows you to use the IFS application. Signing and encryption certificates are security certificates which protect the electronic data exchanged by IFS network members.



Message data encryption

Money order messages are sent as XML files. The sensitive portion of the files, containing the details about the money order purchase or payment, is encrypted, while the non-sensitive portions that contain routing, clearing and tracking data are in clear text.

Each message generates an acknowledgment, which is also digitally signed. This acknowledgment contributes to the non-repudiation aspect of security. The sender cannot deny sending the message, and the recipient cannot deny receiving it.


Routing, clearing, and tracking information is in clear text
Sensitive data is encrypted

```
<Purchase>
      <UTCDT Y="2003" M="01" D="22" T="16:05"/>
      <LCLDT Y="2003" M="01" D="22" T="09:05"/>
      <Office Cd="JP10980" Nm="Tokyo city center post office"/>
    </Purchase>
    <OrderDetails
              l="2176">bSp5k8otLMTXM0k4Qp+cmFvLjc5UGN5/34m0M2bad0YsEUavem/eZNUkgeCZjjLY0RfJomRwchsnKQh05XK
              N1nUYPiTr3X/9Mg2AtCKqHGoG4BSRWE2JQIH0qQxdW2dkjn5KiuYeXiluUb4btG9sN6ttmakK3U+X1qwX1feZk0pGhPcs
              l+G667GIj730dAJ3W5BX3hwrcXcMEWbLbWoUb0j+cagbZhusTwFyfHmR+ethPwND2nHwjqab+LrA4qMmKkskjq/wSs4t
    </OrderDetails>
```

This encryption occurs on the EDI server in the IFS customer organization. A second layer of encryption is added by the VPN client software/SFTP connection. Depending on whether the customer uses VPN client or a VPN tunnel or SFTP connection, the second layer of encryption occurs either on the EDI server or on the firewall (for more information about VPNs and firewalls, see “Virtual Private Networks" on page 10). In either case, the sensitive portion of the money order data is encrypted twice as it transits the Internet.

Public key and private key encryption

Each network member has a public encryption key and a private encryption key. The private key is the decryption and signing key that exists only on the EDI server in your network. This key is what guarantees to your partners that a message did in fact originate from you. Only the IFS software has access to this key. The public key is the key to the algorithm used to encrypt sensitive data in money order messages.

Revocation alerts

An organization suspecting a security breach can issue a revocation alert. For example, if a private key has been lost because of a system failure or is suspected of being altered or stolen, the organization should contact the Postal Technology Centre. The PTC immediately revokes the encryption key and notifies all partner organizations. After a revocation alert, the postal organization may be unable to send or receive money orders for several days while the situation is being investigated.

Stored data protection

The confidentiality of sensitive data (i.e. user login credentials, domestic money order data) stored in the IFS database is supported via a symmetric encryption mechanism using the Advanced Encryption Standard (AES) algorithm. In this way, it is protected from those who have authorized (or unauthorized) access to the database for other purposes (i.e. operation, administration, maintenance).

In addition to using encryption to protect domestic money order data, its integrity is reinforced by means of an electronic signature, which uses an HMAC (Hash-based Message Authentication Code) function.

Symmetric encryption and electronic signatures are only effective at the application-level in raising the bar to protect stored data. They need to be complemented by other technical, physical and procedural measures, which are responsibility of the customer.

User activity monitoring

All important activities of IFS users (i.e. login/logout, money order manipulation, password changes, etc.) are logged. In the event of a security breach, this log could be used to accurately trace and investigate the incident. It is also protected from modification by a cryptographic hash function.

Security audit task

A security audit task detects anomalies in IFS related to security. It verifies the integrity of the activity monitoring logs, as well as the license and encryption certificates currently used by the IFS installation. This task is scheduled to run automatically in the background, using the IFS management console.

Monitoring dashboard

A monitoring dashboard is made available via the IFS web interface to administrators as an additional tool to monitor the health of the IFS system. It provides information on any security alert raised by the security audit task, as well as license validity and expiration, database activity, the status of batch processes, user activity, basic money orders statistics, and the certificate synchronization process.

System manifest

The system manifest is a file (manifest) that can be generated by IFS administrators using the IFS management console, for the purpose of providing PTC support with detailed information about the general health of the IFS system. This manifest includes; database, money order, security, and PKI information.

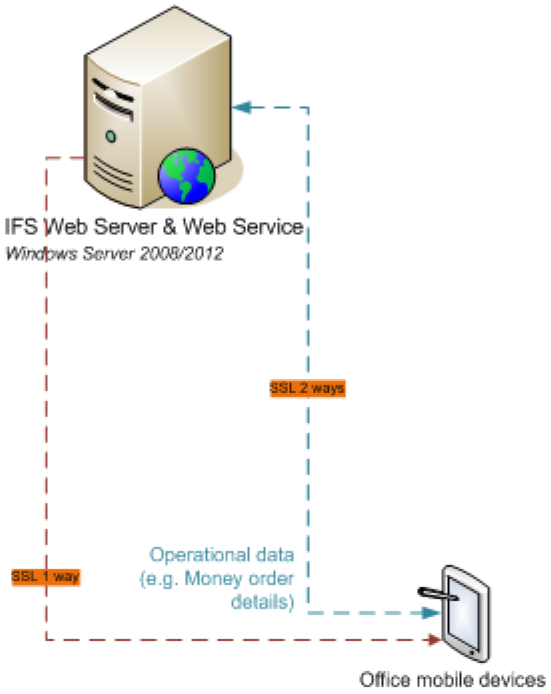
Anti money laundering

Today, most institutions involved in financial transactions are required to identify and report transactions of a suspicious nature to the financial intelligence unit in the respective country. Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) refer to the legal controls in place to prevent or report money laundering or suspicious terrorism funding activities. IFS provides several mechanisms to comply with these legal controls.

Mobile application

1) Send a certificate request for enrollment of the mobile device as a trusted device on the IFS server

2) Complete mobile device enrollment by retrieving a certificate from the IFS server


IFS Web Server & Web Service
Windows Server 2008/2012
SSL 2 ways
SSL 1 way
Operational data (e.g. Money order details)
Office mobile devices

The IFS Mobile App component is an Android application for mobile devices that can be used in IFS. The mobile device must first be enrolled and activate by an IFS administrator before being used. The enrollment process uses 1-way SSL to generate the request. Once the device is enrolled and activated, a certificate is downloaded by the device and all the operations are done using 2-way SSL.

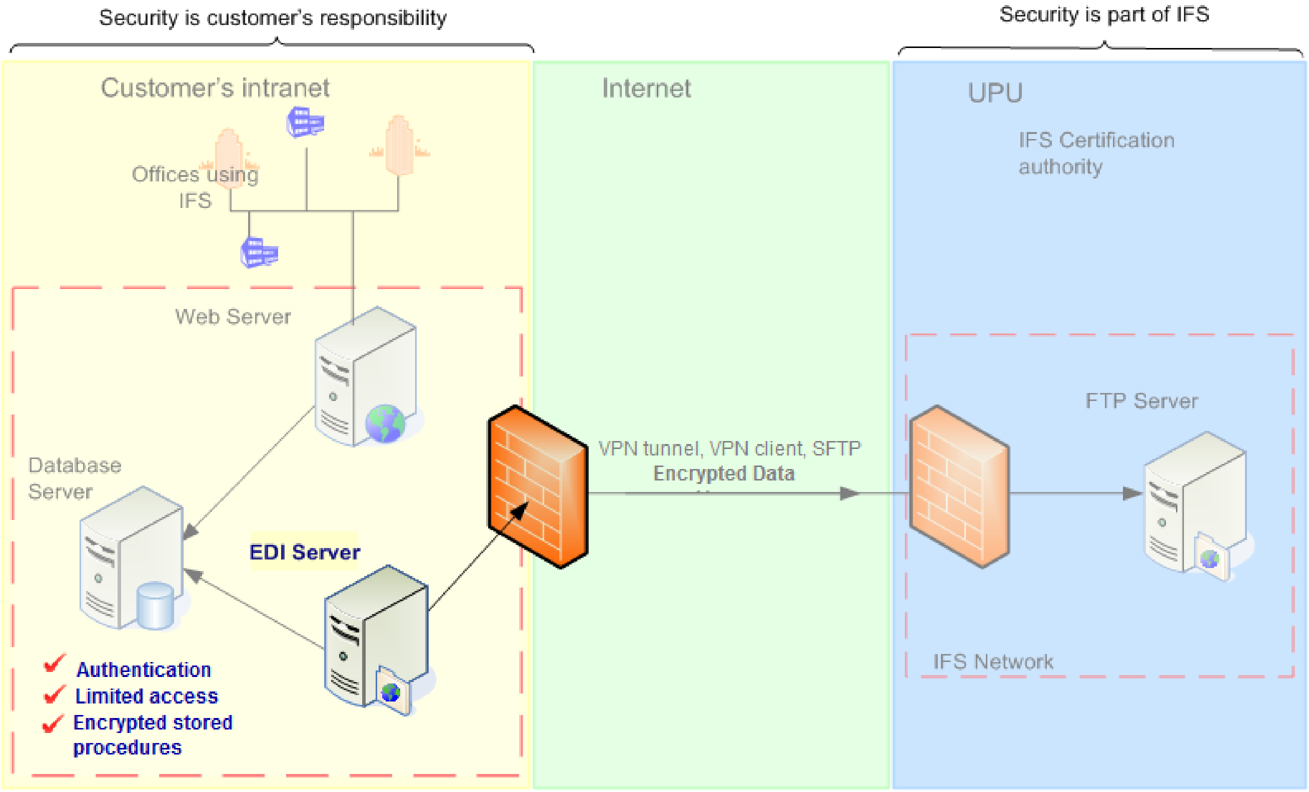
❗ To be able to use the mobile application, the IFS server must be accessible outside via its public name (FQDN - http://www.altospam.com/glossaire/fqdn.php).

Security in the Customer's infrastructure

In addition to the security in IFS, each organization is responsible for the protection of its network against attacks from inside or outside the organization. On each of the three IFS components, there are certain security measures that must be in place. IFS was designed to be flexible in order to meet the needs of many different kinds of organizations. Rather than forcing organizations to adapt to any particular structure for their networks, IFS can function safely within any organizational structure that is adequately secured. This section describes some basic security concepts as they apply to each component of IFS and provides some suggestions on how they can be implemented successfully.

Security on the EDI server

Money order messages are digitally signed and encrypted on the EDI server. The messages are uploaded from the EDI server to the FTP server at the UPU. In the case of organizations that use a VPN client configuration, the VPN software resides on the EDI server. The EDI server communicates with the FTP server at the UPU by means of a VPN tunnel, VPN client or SFTP connection.



Firewalls

A firewall is a security device on a network that controls and filters traffic. Firewalls work by accepting or rejecting traffic based on certain attributes like the source IP address, source port, destination IP address, protocol, or domain name of the source ("source" in this case always refers to the initiator of the contact). User-defined parameters specify which protocols from a given source, such as the Internet, can access a specific destination, such as a workstation in your network. For example, a common firewall configuration rejects all protocols when the source is the Internet and the destination is a user's computer, but allows HTTP and FTP when the source is the workstation and the destination is the Internet.

There must be at least one firewall in your network. The simplest configuration is one in which all IFS users in the organization are on a Local Area Network (LAN). Often organizations have Wide-Area Networks (WAN) or geographically separated sites connected by dedicated or leased lines. If your company's organization consists of multiple LANs or WANs, you will need a firewall at each point traffic enters and exits the network.

How you set up a firewall depends on the kind of firewall you use and the specific purpose of each firewall. Setting up a firewall is usually the responsibility of the network administrator and may be governed by corporate or governmental regulations.

Secure File Transfer Protocol

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as **SSH File Transfer Protocol**.

Virtual Private Networks

A Virtual Private Network (VPN) is a private communications network used to communicate confidentially over a publicly accessible network. A VPN is a required component of every IFS configuration. Every customer must have a VPN account with the UPU. For security reasons, this account can be monitored and invalidated if necessary. Only VPN traffic can enter the FTP server on the IFS network. Two VPN configurations are possible: VPN Client and VPN tunneling.

With a VPN client configuration the VPN software is installed on the customer EDI server. In this configuration, encrypted money order data goes from the EDI server directly to the UPU firewall, passing through the customer's firewall. Your firewall must be configured to allow encrypted traffic.

This configuration may not be suitable for all organizations because it means encrypted data is transiting your network (in both directions) between the EDI server and the firewall. It is possible to see that there are encrypted packets on your network but the contents cannot be monitored.

A VPN tunnel refers to a configuration where the VPN software is installed on your company's firewall. The VPN tunnel is a firewall-to-firewall configuration. The end point is always another firewall. In this case, it is the firewall at the UPU. The VPN tunnel allows encrypted data to pass through the firewall.

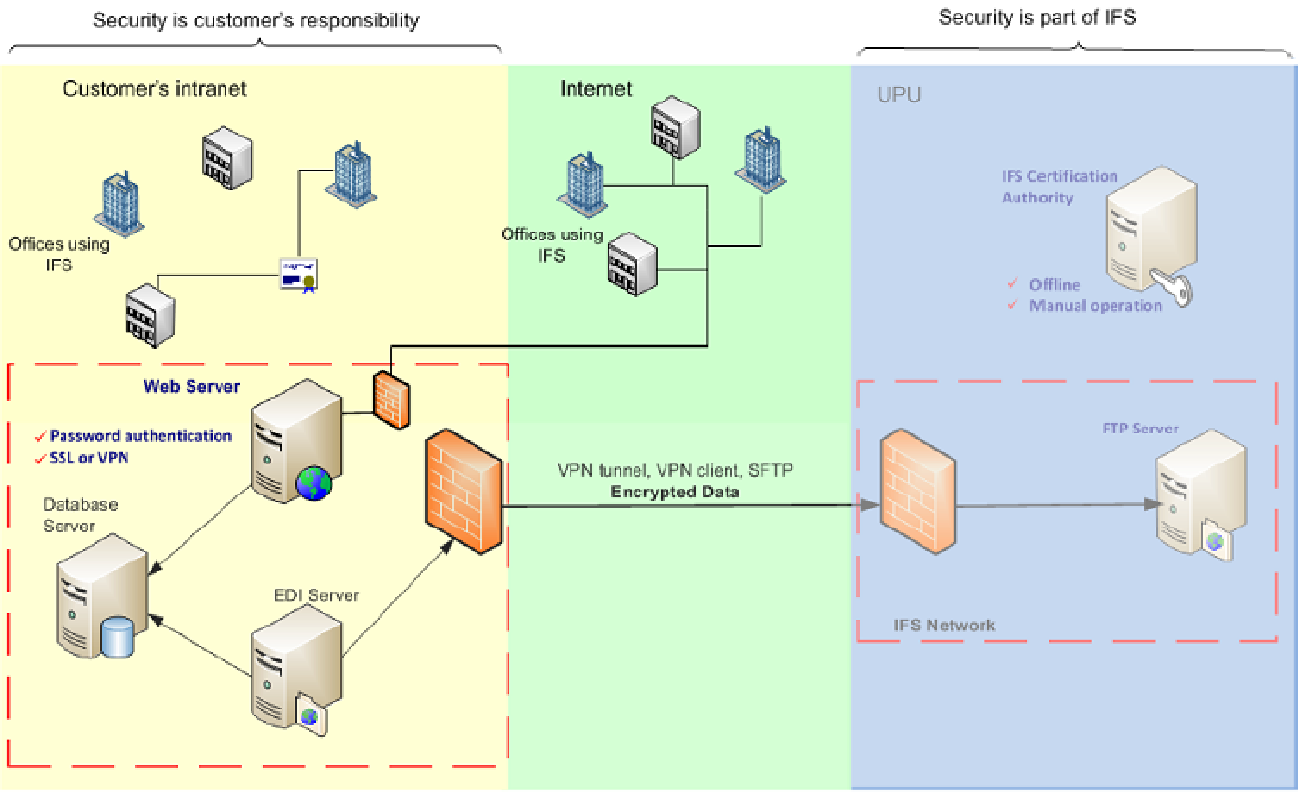
The VPN works by further encrypting money order messages in addition to the encryption that takes place within IFS. This second encryption means that the sensitive data is encrypted twice as it transits the Internet. The VPN encryption is removed by the VPN at the destination. (The partial encryption of the sensitive money order data can only be decrypted by the partner country with their private key. See "Public key and private key encryption" on page 7.)

To set up a VPN, you must first decide whether you will use a VPN client or VPN tunnel configuration. The client version of the VPN software used by the UPU, VPN-1 from Check Point Software Technologies Ltd., is available free of charge from www.checkpoint.com or from the Postal Technology Centre.

Security on the web server

The web server is where the IFS software is installed. Users in the customer's organization access IFS Web application using a web browser such as Microsoft's Internet explorer. Mobile device users access the IFS API Web services publicly available on the same web server. This is the server that is the most vulnerable to attacks from within your organization, and can also be vulnerable to attacks from the outside if adequate protection is not in place using measures such as firewalls.

How you secure your web application depends on the IT infrastructure of your organization. If all potential users of the system are inside the same adequately protected intranet, the UPU recommends a configuration that uses SSL in one of four possible configurations. However, if client workstations will access the web application from outside your intranet—in other words, over the Internet, the client workstations should access the web application using a VPN on a firewall. Both approaches are explained in more detail later in this section.



Password authentication

As with many applications, users must log on to IFS with a user ID and password. In addition, if users will access the Web application using a VPN, each user also logs on to the VPN client with a user ID and password.

All IFS users in your organization must be defined in IFS. Users must also be assigned to one or more IFS user groups. Users can only access functions associated with the user group to which they are assigned. A password is the first defense against unauthorized access, but is only one aspect, as passwords can be stolen or guessed.

In the IFS web application a banner informs users of the last time they logged in, and/or if there have been any failed login attempts using their username since the last time they logged in. In the case of a suspected security breach to the password authentication mechanism, users should immediately contact their IFS system administrator to investigate the incident.

User groups are defined in the IFS Management Console Application. The individual user IDs and passwords are defined from a window in the client IFS application. Only IFS system administrators can access these functions.

If your configuration uses the firewall with VPN, you define the user IDs and passwords using the VPN software on your firewall.

Four levels of security using SSL

The security configuration that best meets your needs depends on several factors such as the size and infrastructure of your network, the configuration of your IFS offices and corporate or government regulations. It is each customer's responsibility to ensure that the necessary security is in place.

IFS, like most applications that run in a browser, uses HTTP, a protocol that is familiar to Web users. The HTTP protocol was designed to allow content to be read easily but is not a protected protocol. To provide the security necessary for safe posting of sensitive data, the web server hosting IFS must use SSL. HTTP used in conjunction with SSL is known as HTTPS. SSL provides encryption and addresses the integrity, confidentiality and authentication security goals.

The IFS application software runs in IIS (Internet Information Services) in Windows, which supports SSL. SSL uses digital certificates, similar in concept to the ones used in IFS. The server—in this case the Web server—presents a digital certificate, which the browser must verify. The browser will only trust the certificate that was issued by a certification authority whose certificate is part of the trusted certification authorities repository on the local machine. The browser also checks whether the domain name of the web site matches the domain name in the certificate. A mismatch indicates a possible security breach. For example, the request may be coming from a fake server to which a hacker is attempting to redirect traffic.

IFS supports four possible levels of security using SSL:

- One way SSL
- One way SSL plus limited static IP addresses
- Two way SSL
- Two way SSL plus smart cards or USB tokens

Each level provides an additional layer of protection.

One way SSL

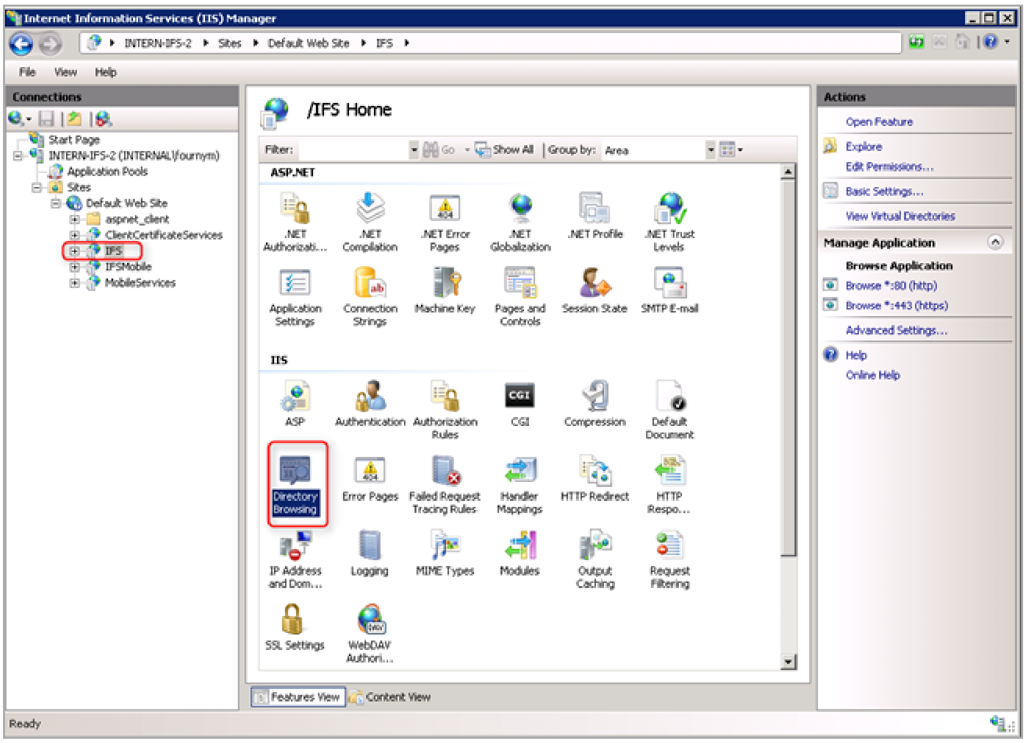
In one way SSL, it is only necessary for workstations to trust the server. One way SSL is the minimum requirement for security on the web server with IFS. You can configure IFS to run over SSL by obtaining an SSL certificate from a public root certification authority (CA). Root CA certificates are included by default in most common web browsers (i.e. Internet Explorer, Firefox, Safari, Opera, Chrome).

In Microsoft's Internet Information Services (IIS) web server, you can create an SSL certificate request and install the certificate using the Web Server Certificate Wizard, which you can access from the "properties" section of your IFS Website.

One way SSL plus IP address restrictions

One option for additional, increased security is the possibility of using static IP addresses on the workstations and limiting access to the IFS Web application to only these IP addresses. Static IP addresses are not feasible for all situations because they may be vulnerable to spoofing, where a hacker manipulates the data to make it appear that it originated from a different machine.

You can define the IP addresses that can access the IFS Web application using the IIS management console. Open the properties page of the IFS application under the default web site. Click the **Directory Security** tab and click the **Edit** button in the IP address and domain name restrictions section.



Two way SSL

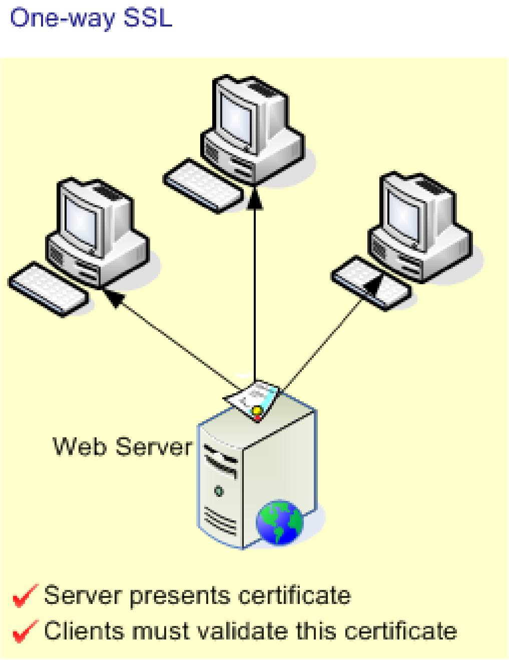
In two way SSL authentication takes places on the server and workstations. Clients (workstations running IFS) also present certificates which must be trusted by the server. The server only accepts requests from workstations whose certificates were issued by a trusted certification authority.

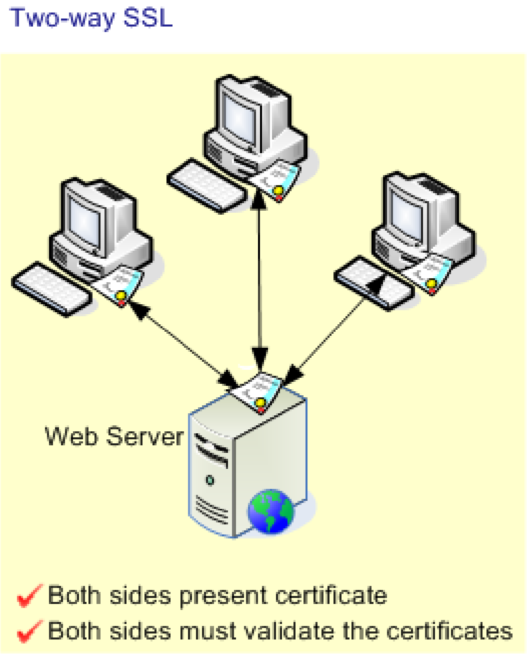
Two way SSL provides increased security, but it also adds a significant operation overhead, since certificates are then required for every workstation connecting to the IFS Web application.

For more information about certificates, you can either contact a private company (Verisign) or use a free certification authority (https://letsencrypt.org/).

Two way SSL plus smart cards or USB tokens

An additional option, to raise the security bar further, is to store client certificates on smart cards or USB tokens. These devices are portable and protected with a password. The SSL certificate is stored on the smart card or token. For authorized access to the Web site, the user must both connect the smart card or USB token and enter his or her individual password.

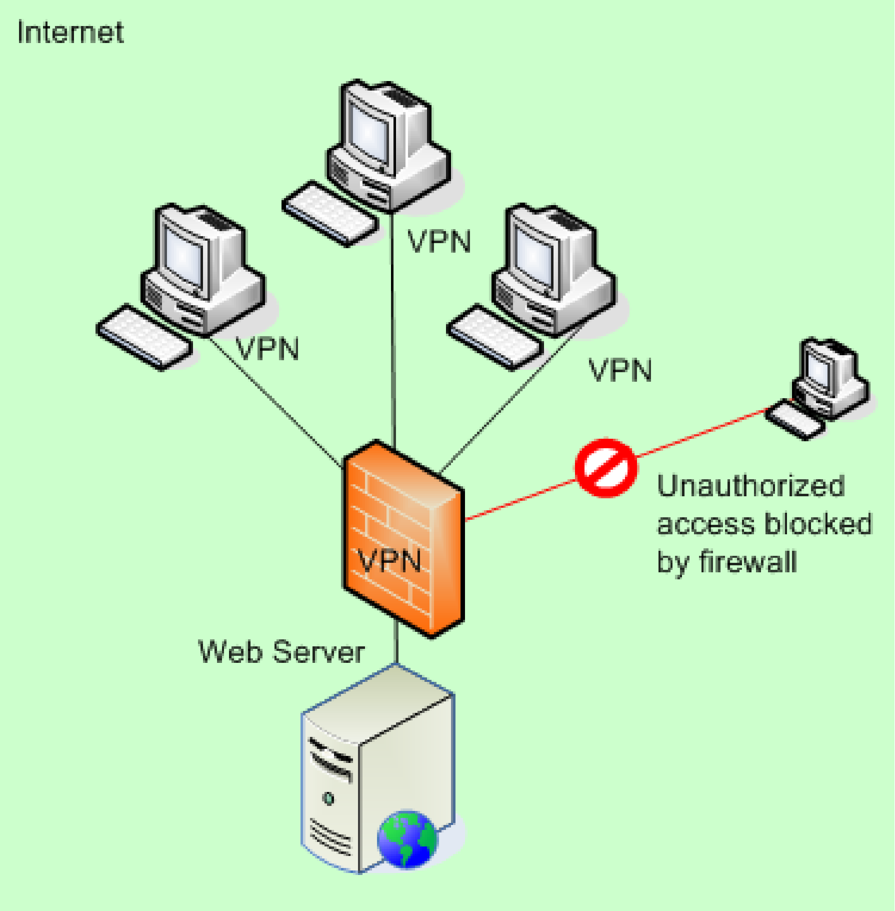

One-way SSL
Web Server
✓ Server presents certificate
✓ Clients must validate this certificate


Two-way SSL
Web Server
✓ Both sides present certificate
✓ Both sides must validate the certificates

For more information about smart cards and tokens, contact a supplier of this technology. Suppliers include SafeNet and Aladdin.

Using VPN to protect the Web application

If you have users in remote offices that will access the IFS Web application over the Internet, the UPU recommends a different approach. If some of your users are not behind a firewall the recommended configuration is to route traffic from the Internet through a firewall running a VPN.



This configuration does not use SSL. Access to the IFS Web application is limited to authorized VPN users. Each workstation has a user account and password which it uses to log on to the Web application. Traffic between the workstations and the server is encrypted.

If the IFS Web services component is also used with a public address to be accessed by mobile devices, you can use a site different than the default site for the IFS Web component. You can also configure different ports and sites per component to use VPN only for the IFS Web application.

For more information about VPN, verify if your router/firewall offers the service or use a free VPN service like OpenVPN (https://openvpn.net/).

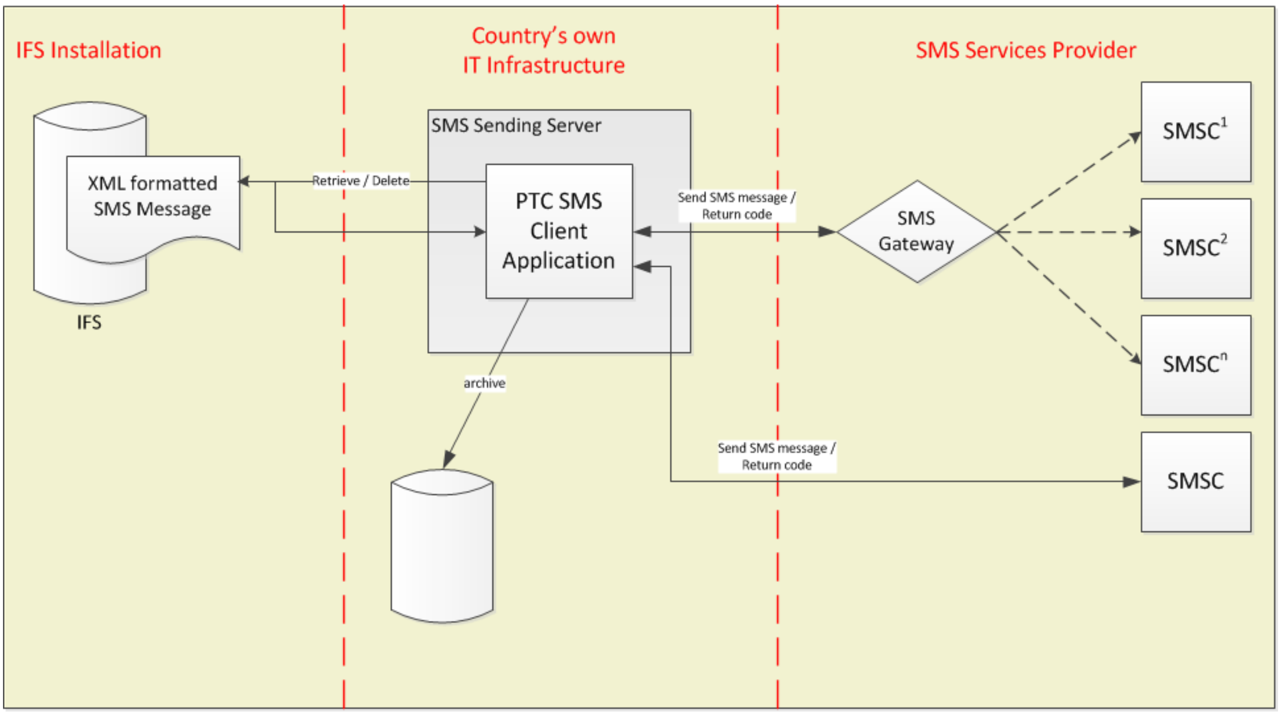
Using Windows Authentication

A last option is to restrict access to IFS Web application to a limited set of Windows users through the authentication and authorization management module of IIS Management Console. This configuration is strongly advised when users of each office are already configured on the network with an Active Directory account.

For more information on authentication and authorization management, see the IIS documentation on Microsoft's TechNet Library (https://technet.microsoft.com).

Securing the link between the IFS installation and the local SMS Gateway application

The following diagram shows how the IFS Web Server links to an SMS services provider through an SMS Gateway.


IFS Installation
Country's own IT Infrastructure
SMS Services Provider
XML formatted SMS Message
IFS
Retrieve / Delete
SMS Sending Server
PTC SMS Client Application
Send SMS message / Return code
SMS Gateway
SMSC^1
SMSC^2
SMSC^n
archive
Send SMS message / Return code
SMSC

The SMS receipts are generated on the IFS Web Server, in the following file structure:

SMS

SMS\Receipt

SMS\Receipt\International

SMS\Receipt\International\Issued

SMS\Receipt\International\Paid

SMS\Receipt\International\Reimbursed

SMS\Receipt\Domestic

SMS\Receipt\Domestic\Issued

SMS\Receipt\Domestic\Paid

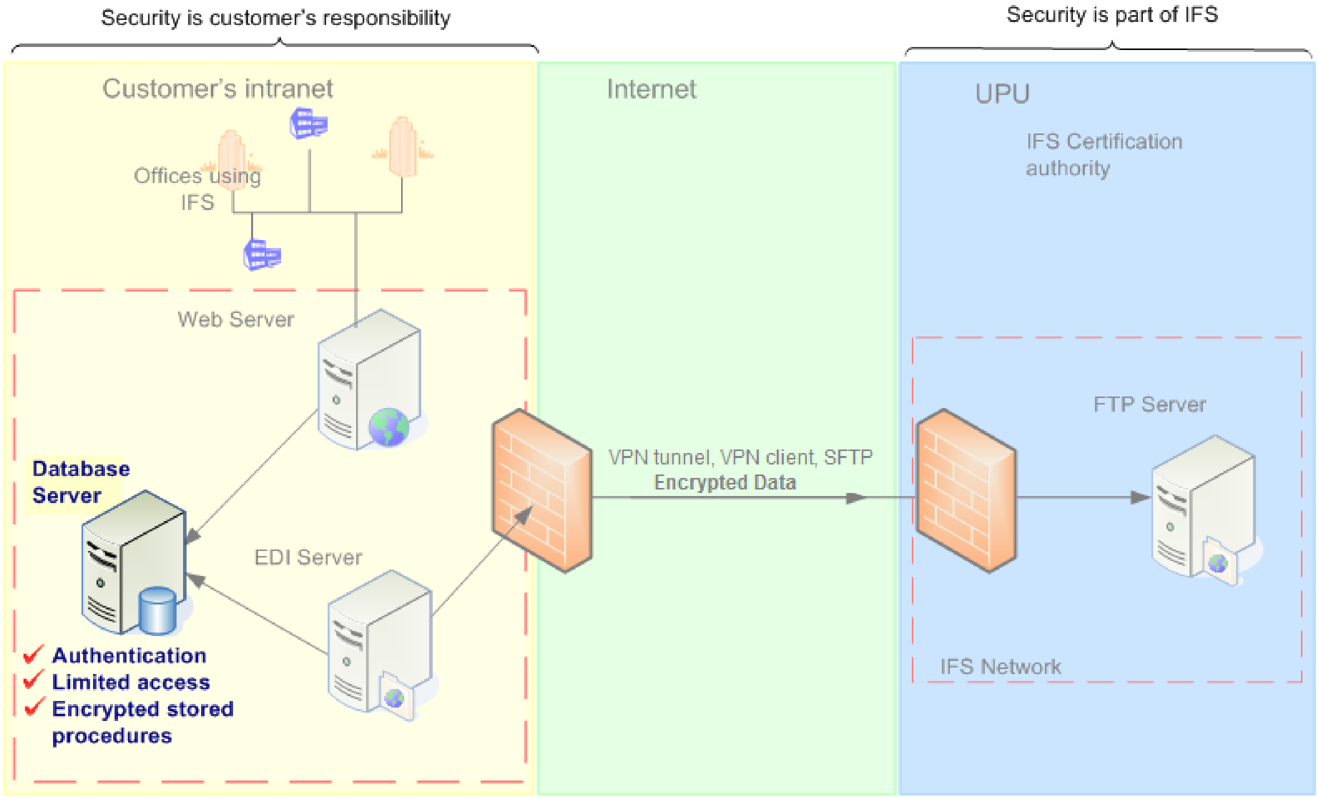
SMS\Receipt\Domestic\Reimbursed

It is the customer's responsibility to restrict access to these folders to the relevant users. This would normally be the IFSUser user and the user of the SMS Sending Server provided by the customer as shown in the diagram above.

Security on the database server

In addition to the built-in data protection mechanisms mentioned in the previous section, there is an additional responsibility on the customer side as money order data is stored on the IFS database server in an SQL database. The IFS production database contains the data for all current money orders and associated tracking information. Most organizations also have an archive database that contains information about transactions that have been finalized.

The database server should be further protected by authentication and by limiting database access to the stored procedures in the IFS database. Administrative access to the database should normally be limited to the IFS system administrator(s).



The Microsoft SQL Server application must be installed on the server that will host the database server. The best option for performance is to use this server only to host the IFS database, but this is not a requirement. This machine hosting the database can also function as the EDI server or Web server.

Authentication

The IIS service on the Web server uses a specific login account to access the IFS database. There are two possibilities for authentication, SQL Server authentication or Windows authentication. The authentication method depends on whether the database server and Web server are on the same machine or different machines. Windows authentication can be used only if the database server and Web server are the same machine or domain. Windows authentication refers to a user ID and password that is defined in Windows. This is a specific ID that is used only by IIS to access the database.

With SQL authentication, the user ID and password used to connect to the database are defined in SQL. This ID and password can be created at the same time IFS is installed or can be defined in SQL Enterprise Manager before installation.

It is important to understand that these logins are not the same logins used by users to access the IFS system. These are special logins that are used only by the web server to access the database.

In addition to managing access at the database level, the SQL Server application uses roles to allow or deny access to specific functions. A role is a group to which individual logins/users can be added, similar to a user group. During installation, IFS creates a role "IFSUsers" and automatically assigns to it the Windows login or the SQL login you created. The only task this role can perform is running the IFS stored procedures.

Stored procedures

Stored procedures are pre-compiled programs that run on a database. IFS uses hundreds of stored procedures. These stored procedures are encrypted. Stored procedures typically capture business processes and manipulate data. In IFS, for example, many stored procedures write information to the IFS tables. Tables in the database can only be modified by the stored procedure. No function, such as modifying a table containing money order data, can be performed manually unless a user is assigned to a role which permits this. The only person capable of creating such a role is the system administrator.

Security on the web clients

Most browsers provide a multi-tabbed browsing feature. Unless your business requires this feature for other applications using the same browser, we recommend turning it off. The reason is that a recent type of exploit called Cross Site Request Forgery (CSRF) could make use of the multi-tab feature for malicious purposes.

The IFS web application already has built-in protection against this type of vulnerability, but attacks always evolve so we recommend disabling multiple tabs.

To disable multi-tabbed browsing on Internet Explorer 8, select **Tools > Options > General > Tab Settings**, and uncheck the **Enable tabbed browsing** check box.

Security on your IT infrastructure

Security updates

Security updates, bug fixes and patches are released by operating system and application software vendors regularly. These patches are often the result of the discovery of vulnerabilities in the software or infiltrations by malicious software such as viruses.

Microsoft Windows updates and patches should be regularly applied to all IFS machines, IFS web clients should run the latest versions of your browser of choice.

You may have applications running on the same machines or network as IFS that could be targeted by malware, for example, Java, Quicktime, RealPlayer and Adobe Reader. These applications should also be regularly updated, or uninstalled if they are not used.

Antivirus and anti-malware protection

Malware that could affect IFS includes: spyware (key loggers), worms, Trojan horses, rootkits or computer viruses. It is vitally important that you protect your computer systems with an antivirus solution. Some of the leading providers of antivirus software are: Norton/Symantec, McAfee, Panda Security, Avira and Kaspersky Lab.

Where to go for more information

Documents and Web sites

Documents available from the Postal Technology Centre:

- *IFS Installation Guide*
- *Working architectures for VPN security*

Recommended web sites:

update.microsoft.com

www.microsoft.com/security

www.firefox.com

www.opera.com

www.apple.com/safari

www.checkpoint.com

www.thawte.com

www.geotrust.com

www.pandasecurity.com

www.mcafee.com

www.symantec.com

www.avira.com

www.kaspersky.com

www.safenet-inc.com

https://openvpn.net/

https://letsencrypt.org/

https://technet.microsoft.com

Glossary

AES Advanced Encryption Standard

The Advanced Encryption Standard is a symmetric encryption cipher that was adopted by the US National Institute of Standards in 2001. AES ciphers have been analyzed extensively and are now used worldwide.

Authentication

The process of verifying the digital identity of the sender of a communication and the assurance that data comes from the source which claims to be sending it.

Availability

The process of ensuring that data is protected against destruction and that the data, system or service is available.

CA

Certification Authority. An organization that issues and manages security credentials and public keys for message encryption. A CA may be a public service whose business is to issue certificates for a fee, or it can be a private service within an organization that the company maintains for the purpose of managing its own certificates.

Confidentiality

Assurance that information is accessible only to those authorized to have access.

Cross Site Request Forgery (CSRF)

A malicious infiltration of a website whereby unauthorized commands are transmitted from a user that the website trusts. Common CSRF attacks happen from scripts running on parallel tabs of a user’s browser, riding on a session that the user has opened on a separate tab.

Database server

The machine in a customer's intranet that hosts the IFS database.

Digital certificate

An electronic credential that it used to verify that a website is the site that it claims to be. Certificates are issued by organizations known as Certification Authorities. The job of the Certification Authority is to verify that that the certificate belongs to the organization noted in the certificate.

EDI

Transfer of data between different companies using a network or the Internet.

EDI server

The machine in a customer's intranet that encrypts EDI messages and sends them to the UPU's FTP server.

Firewall

Device or software configuration that protects the resources of a private network from users from other networks. A firewall is usually a configuration on a server, but can also be on a router. Hardware-based firewalls also exist.

FTP

File Transfer Protocol. A standard Internet protocol used to exchange files between computers on the Internet. FTP is commonly used to download programs and other files to a computer from other servers.

FTP server

The server in the IFS network that receives encrypted EDI messages containing money order data.

HMAC

Hash-based Message Authentication Code is a specific construction for calculating a signature involving a cryptographic hash function in combination with a secret key.

Hardware Security Model (HSM)

A HSM is a hardware-based cryptographic device designed to generate, store, and protect cryptographic keys.

Hash-based Message Authentication Code

Hash-based Message Authentication Code is a specific construction for calculating a signature involving a cryptographic hash function in combination with a secret key.

Integrity

Assurance that information can only be accessed or modified by those authorized to do so.

Internet

Worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

Internet Information Services (Microsoft IIS)

The commercial web server application where the IFS web application is hosted.

Intranet

A private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet.

IP address

The number that identifies each sender or receiver of information that is sent in packets across the Internet.

Keylogger

Software that tracks (or logs) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. In the context of an IFS web client, a user's credentials (i.e. username and password) could be stolen through this mechanism.

Malware

Short for malicious software is software designed to perpetrate a malicious act, infiltrating a computer system without the owner's informed consent. The expression is a general term used to refer to a variety of hostile, intrusive, or irritating software or program code.

Non-repudiation

The assurance that the sender of data cannot deny having sent the data and the recipient cannot deny having received it.

Private key

An encryption/decryption key known only to the party or parties that exchange secret messages.

Protocol

Special set of rules used by computers to communicate with each other across a network.

Public key

An encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.

Rootkit

A software system that consists of one or more programs designed to obscure the fact that a system has been compromised. An attacker may use a rootkit to replace vital system executables.

Spyware

A type of malware that is installed on computers and collects information about users without their knowledge. Keyloggers are a type of spyware.

SFTP

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as **SSH File Transfer Protocol**.

SSH

SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary. There are several ways to use SSH; one is to use automatically generated public-private key pairs to simply encrypt a network connection, and then use password authentication to log in.

Another is to use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password. In this scenario, anyone can produce a matching pair of different keys (public and private). The public key is placed on all computers that must allow access to the owner of the matching private key (the owner keeps the private key secret). While authentication is based on the private key, the key itself is never transferred through the network during authentication. SSH only verifies whether the same person offering the public key also owns the matching private key. In all versions of SSH it is important to verify unknown public keys, i.e. associate the public keys with identities, before accepting them as valid. Accepting an attacker's public key without validation will authorize an unauthorized attacker as a valid user.

SSL

Secure Sockets Layer. Commonly used protocol for managing the security of a message transmission on the Internet.

Trojan horse

Malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.

Virus

A computer program that can copy itself and infect a computer. Classic computer viruses are capable of destroying an entire operating or file system.

VPN

A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Web server

The machine in your organization on which the IFS application is installed.

Worm

A self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention. If a worm infects one of your IFS clients, it could replicate through your network to all your other clients, and even infect your servers.

XML

Extensible Markup Language. XML is a flexible set of rules for encoding documents electronically. It allows documents to be created in a common format so that information can be shared on the World Wide Web, intranets and elsewhere.