International Financial System

Manuel de sécurité

Contact

Postal Technology Centre - Universal Postal Union Weltpoststrasse 4 3000 Bern 15 - Switzerland

Tél. : +41 31 350 31 11 / Fax : +41 31 352 43 23

E-mail : ptc.support@upu.int

Table des matières

A propos du présent guide

Public visé

Le présent guide s'adresse aux administrateurs du système réseau d'IFS ainsi qu'aux membres du CTP de l'UPU chargés de garantir la sécurité dans le cadre de l'installation et de la mise en œuvre des systèmes réseaux d'IFS.

Comment utiliser le présent manuel

Le présent manuel offre des conseils pratiques relatifs à la sécurisation des informations et services d'IFS. Pour obtenir des informations sur :

- la sécurité inhérente à IFS, consultez la section « Eléments de sécurité intégrés dans IFS » en page 8
- les mesures de sécurité qui doivent être mises en œuvre par chaque organisation, consultez la section « Sécurité au niveau de l'infrastructure du client » en page 13
- les ressources offrant de plus amples informations, consultez « Comment obtenir de plus amples informations » en page 25

IFS et sécurité des données

IFS est une application qui automatise le traitement et la gestion des mandats internationaux et nationaux. IFS assure l'échange de données concernant les mandats internationaux entre les organisations émettrices et réceptrices utilisant l'échange de données informatisé (EDI).

Etant donné que le traitement des mandats implique le transfert électronique de grandes quantités de données financières, une sécurité efficace est vitale. L'application IFS combine diverses technologies pour assurer la sécurité de l'acheminement et du stockage des données relatives aux mandats.

De plus, certaines mesures de sécurité doivent être mises en place dans le cadre de l'environnement opérationnel de chaque client pour la protection contre les accès non autorisés. Le présent document explique les mesures de sécurité inhérentes à IFS et fournit des informations de base sur les mesures de sécurité que vous devriez prendre au sein de votre organisation, dans le cadre de votre environnement IFS, pour sécuriser vos données.

Deux types de sécurité

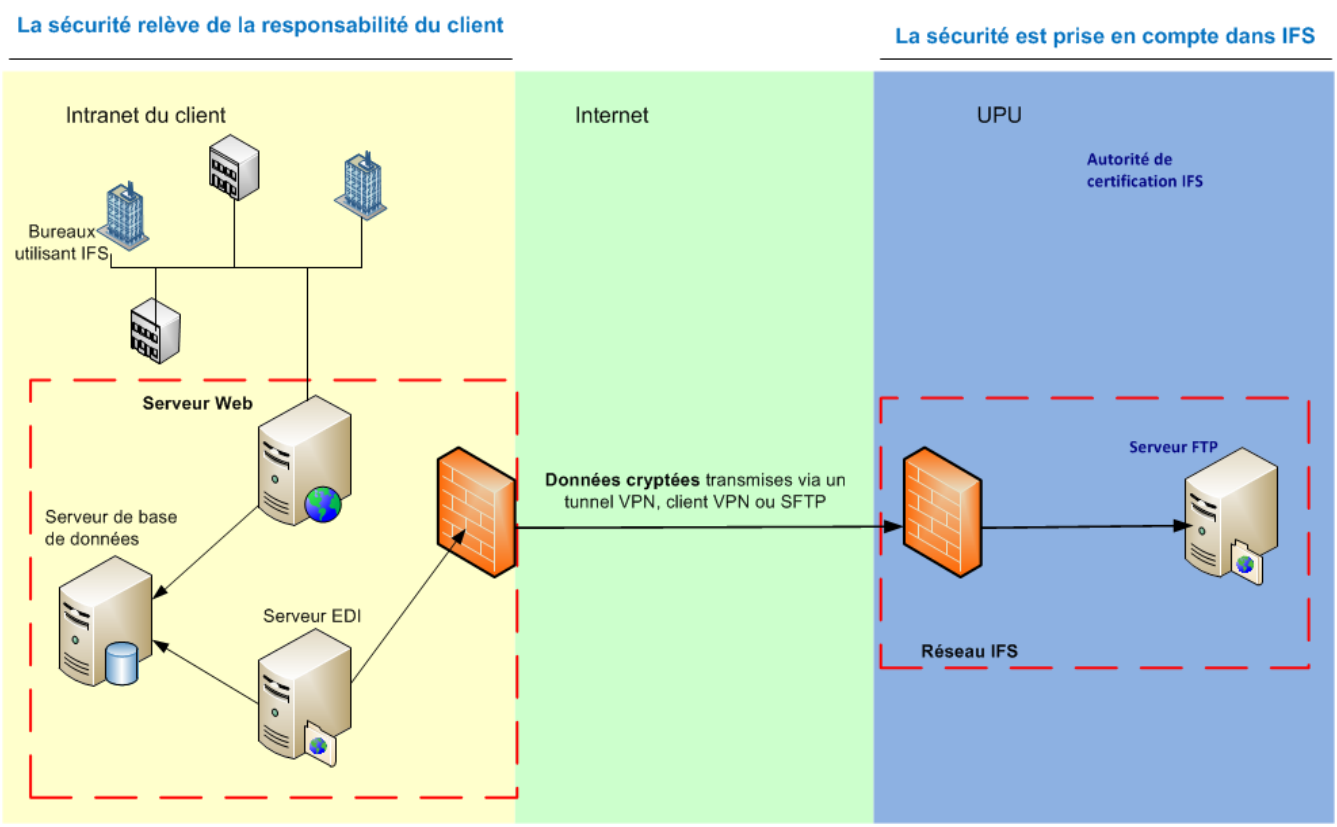
Lors de l'installation d'IFS, deux aspects importants en matière de sécurité doivent être pris en considération. L'un est la sécurité inhérente à IFS. Il s'agit des éléments de sécurité intégrés dans l'application et le réseau IFS et inclus dans toutes les installations de l'application. Le deuxième aspect concerne les mesures de sécurité devant être prises au sein de l'organisation de chaque client. Chaque client IFS est responsable de cet aspect de la sécurité.

Aperçu de l'infrastructure IFS

Les mandats sont créés sur un site client au moyen de l'application IFS. Les composantes de cette application sont installées sur un ou plusieurs serveurs sur l'intranet du client. Les utilisateurs d'IFS accèdent aux fonctions de l'application à partir d'une fenêtre du navigateur. Les données relatives aux transactions sont stockées dans une base de données. Les données concernant les mandats internationaux sont cryptées, signées numériquement et transmises via le réseau IFS. Aucune transmission des données concernant les mandats nationaux n'est requise en dehors de l'intranet du client.

Sur chaque site client, le système IFS est installé sur l'intranet de l'organisation du client. Ce système est composé de trois éléments principaux :

- un serveur Web – la machine sur laquelle l'application IFS est installée ;
- un serveur de base de données – la machine servant à héberger la base de données IFS ;
- un serveur EDI – la machine utilisée pour crypter partiellement les messages concernant les mandats internationaux et les transmettre à l'UPU.



Il est important de comprendre que les composantes présentées dans le diagramme ci-dessus constituent un cadre conceptuel et qu'il ne s'agit pas forcément d'éléments matériels distincts. En pratique, le serveur Web, le serveur de base de données et le serveur EDI peuvent être installés sur des machines distinctes, ou une seule machine peut servir pour deux types de serveurs. Par exemple, une même machine peut servir de serveur Web et de serveur de base de données. Il est cependant possible d'utiliser trois machines distinctes. Le CTP prend en charge un nombre limité de configurations. Celles-ci sont expliquées en détail dans le document intitulé *IFS Installation Guide*. Pour des raisons de sécurité, il est déconseillé d'utiliser une même machine comme serveur EDI et serveur Web. Cela accroît en effet les risques d'accès non autorisé aux données EDI à partir du Web.

Principaux objectifs en matière de sécurité

IFS prend en charge de nombreux types de structures organisationnelles. Il n'existe donc pas de prescriptions particulières en matière de configuration applicables lors de chaque installation. Chaque client IFS est chargé de déterminer la meilleure configuration possible en termes de sécurité du réseau. Tout plan de sécurité doit tenir compte des objectifs de base ci-après.

- *Confidentialité* : garantir que les informations soient disponibles uniquement pour ceux qui sont autorisés à y accéder. La confidentialité des informations échangées entre les parties est ainsi assurée. La confidentialité des données IFS est garantie grâce à l'utilisation d'une connexion VPN (Réseau privé virtuel/SFTP) et au cryptage des données.
- *Intégrité* : garantir que les données originales ne soient ni modifiées, ni altérées, ni détruites, que ce soit accidentellement ou avec une intention malveillante. IFS utilise des signatures numériques pour protéger l'intégrité des données des messages. L'intégrité des données peut être subdivisée comme suit :

    - Authentification : garantir que les données proviennent de la source indiquée.
    - Non-répudiation : garantir que l'expéditeur ne puisse pas nier avoir envoyé les données et que le destinataire ne puisse pas nier les avoir reçues.
    - Transparence : le système peut identifier les actions et le comportement d'un individu particulier dans le cadre du système.
- *Disponibilité* : garantir l'accès à un système, à un service ou à des données, ainsi que la protection de ces éléments contre toute destruction accidentelle ou malveillante, ou contre toute attaque par déni de service. Une connexion VPN/SFTP est utilisée pour protéger le serveur FTP contre les attaques qui pourraient compromettre la disponibilité du réseau.

Différents aspects de la sécurité

En vue de la réalisation des objectifs susmentionnés, il importe d'aborder la sécurité selon une démarche holistique et de tenir compte de ses différents aspects, au-delà de la sécurité technologique.

- Sécurité physique : cet aspect concerne les restrictions d'accès à un emplacement physique. Par exemple, seuls certains employés (comme les administrateurs système) devraient avoir accès à la salle dans laquelle le serveur de la base de données IFS est installé. La sécurité physique englobe aussi les mesures visant à prévenir les vols de documents et la divulgation d'informations. En cas de transaction sur support papier (émission de mandats à partir de bureaux de poste situés dans des régions reculées, par exemple), les documents devraient être archivés en un lieu sécurisé et être détruits au moyen d'une déchiqueteuse.
- Sécurité technologique : l'application IFS intègre de nombreux mécanismes visant à garantir un haut niveau de sécurité. Au niveau de l'infrastructure (navigateurs, systèmes d'exploitation, réseau, etc.), il incombe aux opérateurs postaux de fournir un environnement informatique sécurisé.
- Politiques et procédures : ces éléments devraient être utilisés comme outils pédagogiques pour sensibiliser les employés à l'importance du rôle de chacun en matière de sécurité. Les employés devraient être formés de manière à être vigilants lorsqu'ils utilisent IFS, afin de pouvoir détecter toute tentative de fraude.

Eléments de sécurité intégrés dans IFS

Serveur FTP d'IFS

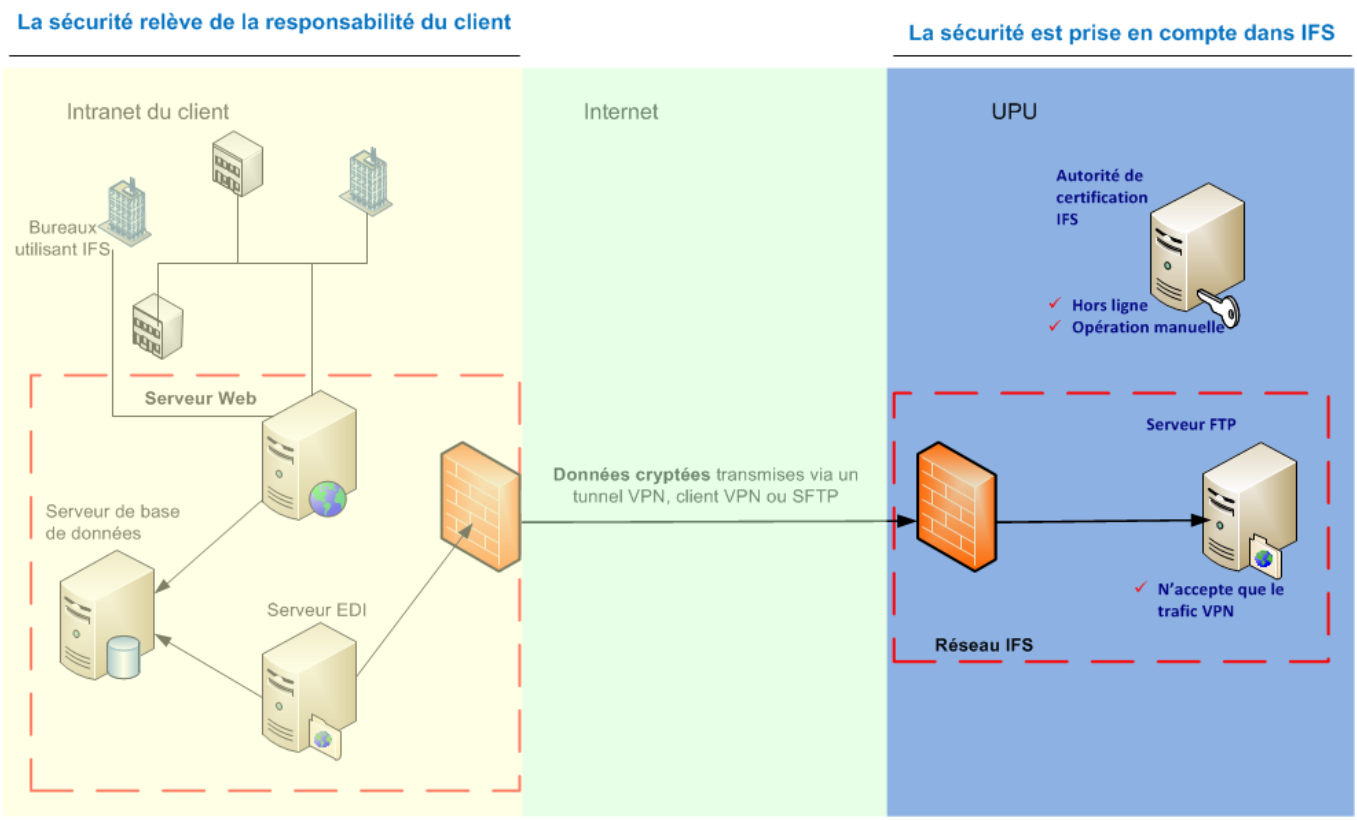
Les pays échangent des données cryptées concernant les mandats via le réseau IFS. Le serveur FTP constitue le principal élément de ce réseau. Chaque organisation membre dispose de son propre répertoire sur ce serveur. Les répertoires sont structurés par produit et par type de produit. Le serveur FTP ne transmet pas de données. Il reçoit les mandats des clients IFS et place les messages dans le répertoire pertinent du pays partenaire.

En outre, les certificats publics sont publiés sur ce serveur, ainsi que les nouvelles demandes de cryptage et de signature et les alertes en cas de révocation. L'accès au répertoire FTP à partir de l'Internet est protégé par un pare-feu, et le serveur FTP n'accepte que le trafic VPN et la connexion SFTP. Chaque utilisateur (dans ce cas, toute organisation utilisant IFS) doit être authentifié sur le serveur FTP pour pouvoir accéder à son répertoire. Une organisation ne peut accéder qu'à son propre répertoire sur le serveur FTP.

Certificats numériques

A l'UPU, le serveur des certificats est la machine hébergeant le logiciel de l'Autorité de certification (AC) qui traite en particulier le cryptage des messages et la signature des certificats pour l'application IFS. Ce serveur contient la clé privée et il s'agit de la seule machine ayant accès à cette clef. Afin d'éviter toute possibilité d'accès non autorisé, le serveur des certificats est une machine autonome qui n'est connectée physiquement à aucun réseau. Les informations sont transférées du serveur AC au serveur FTP hors ligne.

IFS utilise deux types de certificats électroniques pour assurer la sécurité et l'intégrité des données. Le certificat de licence vous permet d'utiliser l'application IFS. Les certificats de signature et de cryptage sont des certificats de sécurité qui protègent les données électroniques échangées par les membres du réseau IFS.



Cryptage des données des messages

Les messages concernant les mandats sont envoyés sous forme de fichiers XML. La partie sensible des fichiers, contenant les détails relatifs à l'achat ou au paiement des mandats, est cryptée, tandis que les parties non sensibles, contenant les données relatives à l'acheminement, à la compensation et au suivi, sont rédigées en texte clair.

Chaque message génère un accusé de réception, qui porte aussi une signature numérique. Cet accusé de réception joue un rôle dans le mécanisme de non-répudiation. L'expéditeur ne peut pas nier avoir envoyé le message et le destinataire ne peut pas nier l'avoir reçu.

Le cryptage est effectué sur le serveur EDI au sein de l'organisation du client IFS. Une seconde couche de cryptage est ajoutée par le logiciel du VPN client/de la connexion SFTP. Selon que le client utilise un VPN client, un tunnel VPN ou une connexion SFTP, la seconde couche de cryptage est ajoutée

soit au niveau du serveur EDI, soit au niveau du pare-feu (pour de plus amples informations sur les réseaux privés virtuels (VPN) et les pare-feu, veuillez vous reporter à la section « Réseaux privés virtuels » en page 10). Dans tous les cas, la partie sensible des données relatives au mandat est cryptée deux fois lors de sa transmission via l'Internet.

Cryptage à clé publique et privée

Chaque membre du réseau dispose d'une clé de cryptage publique et d'une clé de cryptage privée. La clé privée est la clé de décryptage et de signature qui n'existe que sur le serveur EDI de votre réseau. C'est cette clé qui garantit à vos partenaires qu'un message a bien été envoyé par vous. Seul le logiciel IFS permet d'accéder à cette clé. La clé publique est la clé de l'algorithme utilisé pour crypter les données sensibles des messages concernant les mandats.

Alertes en cas de révocation

Une organisation soupçonnant une violation de la sécurité peut lancer une alerte de révocation. Si, par exemple, une clé privée a été perdue en raison d'une défaillance du système ou si l'on soupçonne qu'une telle clé a été altérée ou volée, l'organisation devrait prendre contact avec le Centre de technologies postales. Ce dernier révoque immédiatement la clé de cryptage et en informe toutes les organisations partenaires. A la suite d'une alerte de révocation, l'organisation postale peut être dans l'incapacité d'envoyer ou de recevoir des mandats pendant plusieurs jours, selon la durée de l'enquête menée pour clarifier la situation.

Protection des données stockées

La confidentialité des données sensibles (identifiants de connexion des utilisateurs, données relatives aux mandats nationaux, etc.) stockées dans la base de données IFS est assurée au moyen d'un mécanisme de cryptage symétrique utilisant l'algorithme Advanced Encryption Standard (AES) (Norme de cryptage avancée). Les données sont ainsi protégées de ceux qui accèdent à la base de données (avec ou sans autorisation) pour d'autres raisons (exploitation, administration, maintenance, etc.).

Outre les techniques de cryptage employées pour protéger les données des messages relatifs aux mandats nationaux, l'intégrité de ces données est renforcée au moyen d'une signature électronique utilisant une fonction HMAC (Hash-based Message Authentication Code).

Le cryptage symétrique et les signatures électroniques ne sont efficaces au niveau de l'application que pour renforcer la protection des données stockées. Ils doivent être complétés par d'autres mesures techniques, physiques et procédurales relevant de la responsabilité du client.

Suivi des activités des utilisateurs

Toutes les activités importantes des utilisateurs d'IFS (connexion/déconnexion, manipulation de mandats, changement de mot de passe, etc.) sont consignées. En cas d'atteinte à la sécurité, ces

enregistrements peuvent être utilisés pour localiser précisément l'incident et l'analyser. Ces données sont également protégées de toute modification par une fonction de hachage cryptographique.

Audit de sécurité

L'audit de sécurité sert à détecter les anomalies en matière de sécurité concernant IFS. Il permet de vérifier l'intégrité des registres de suivi des activités, ainsi que les certificats de licence et de cryptage utilisés actuellement pour l'installation d'IFS. Cette tâche est conçue de manière à être exécutée en arrière-plan, au moyen de la console de gestion IFS.

Tableau de contrôle

Un tableau de contrôle est mis à la disposition des administrateurs via l'interface Web d'IFS. Cet outil supplémentaire permet de vérifier le bon fonctionnement du système IFS. Il fournit des informations sur les alertes de sécurité déclenchées par l'audit de sécurité, mais aussi sur la période de validité et la date d'expiration de la licence, l'activité de la base de données, l'état des processus de traitement par lots, les activités des utilisateurs, les statistiques de base concernant les mandats et le processus de synchronisation des certificats.

Fichier d'informations système

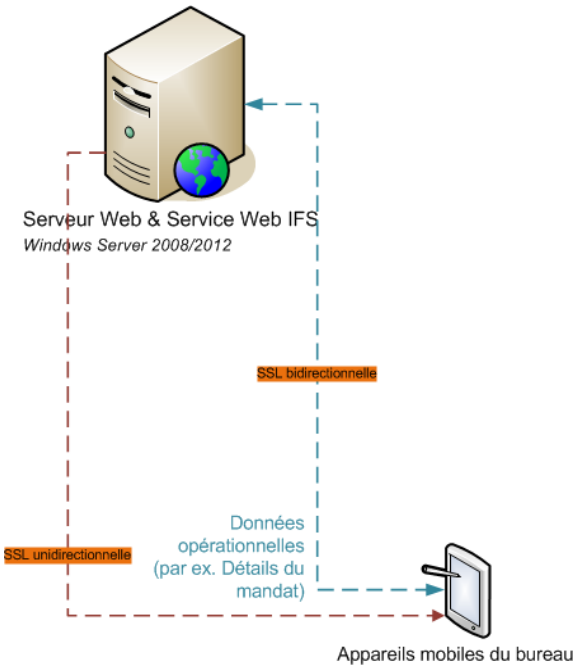
Le fichier d'informations système peut être généré par les administrateurs d'IFS, au moyen de la console de gestion IFS, pour fournir aux services d'appui du CTP des informations détaillées sur l'état général du système IFS. Ce fichier renferme des informations sur la base de données, les mandats, la sécurité et l'infrastructure à clé publique.

Lutte contre le blanchiment d'argent

Aujourd'hui, la plupart des institutions effectuant des transactions financières sont tenues d'identifier et de signaler les transactions douteuses aux services de renseignements financiers dans leur pays respectif. Des moyens juridiques ont en effet été mis en place pour lutter contre le blanchiment d'argent et le financement du terrorisme. IFS comprend plusieurs mécanismes permettant de respecter les dispositions juridiques dans ce domaine.

1) Envoyer une demande de certificat pour enregistrer l'appareil mobile en tant que périphérique de confiance sur le serveur IFS.

2) Terminer l'enregistrement de l'appareil mobile en récupérant un certificat à partir du serveur IFS.



Le composant Application mobile IFS est une application Android destinée aux appareils mobiles qui peuvent être utilisés avec IFS. Avant de pouvoir être utilisé, un appareil mobile doit en premier lieu être enregistré et activé par un administrateur d'IFS. Le processus d'enregistrement utilise une authentification SSL unidirectionnelle pour générer la demande. Une fois enregistré et activé, l'appareil télécharge un certificat et toutes les fonctions s'effectuent au moyen d'une authentification SSL bidirectionnelle.

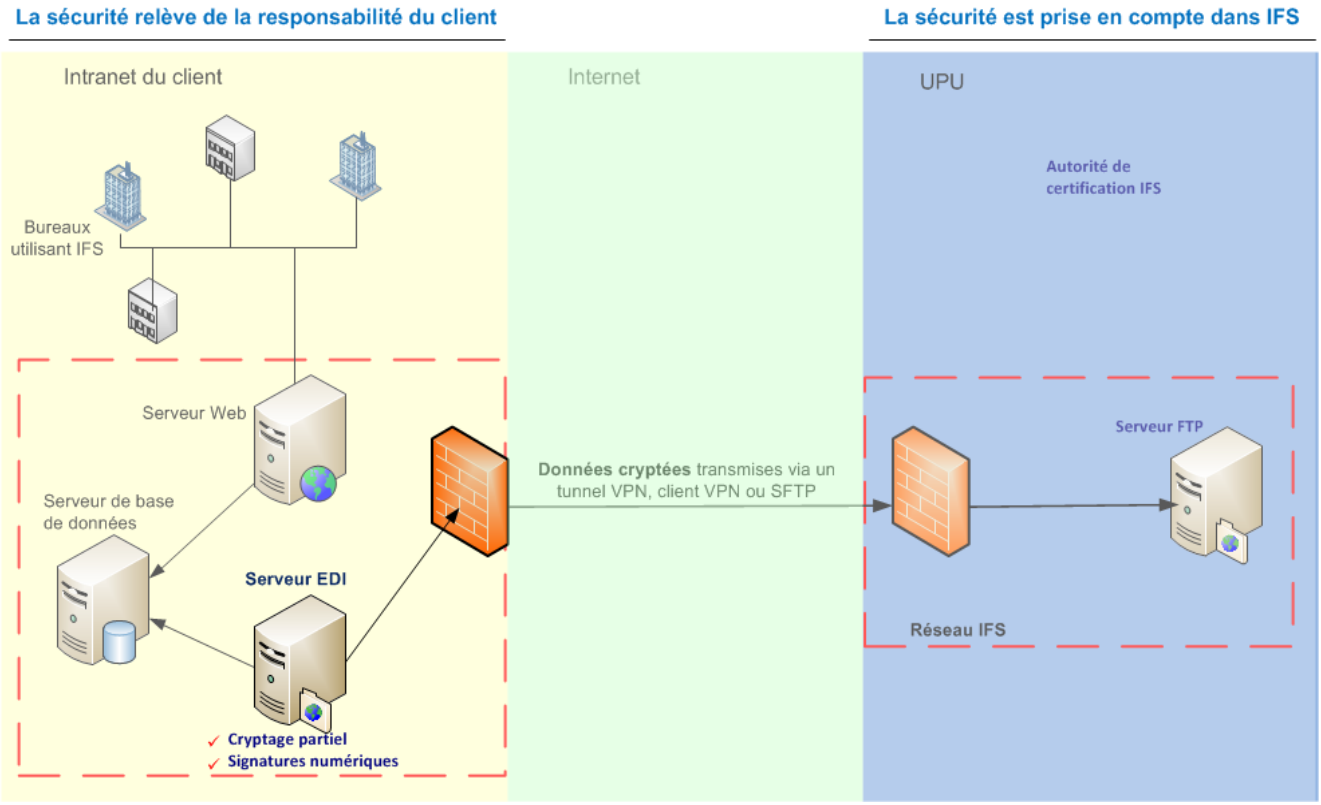
Important : Pour permettre l'utilisation de l'application mobile, le serveur IFS doit être accessible depuis l'extérieur, via son nom public (FQDN - http://www.altospam.com/glossaire/fqdn.php).

Sécurité au niveau de l'infrastructure du client

Outre les éléments de sécurité inhérents à IFS, chaque organisation est responsable de la protection de son réseau contre les attaques lancées de l'intérieur ou de l'extérieur de l'organisation. Certaines mesures de sécurité doivent être prises à l'égard de chacun des trois éléments de sécurité d'IFS. IFS a été conçu de manière à pouvoir être adapté aux besoins de nombreux types d'organisations. IFS peut fonctionner en toute sécurité au sein de n'importe quelle structure organisationnelle suffisamment sécurisée, ce qui évite aux organisations de devoir s'adapter à des structures particulières pour leurs réseaux. La présente section décrit quelques concepts de base en matière de sécurité, ainsi que la manière dont ils s'appliquent à chacune des composantes d'IFS. Vous y trouverez aussi des suggestions sur la façon dont ces concepts peuvent être mis en œuvre avec succès.

Sécurité sur le serveur EDI

Les messages concernant les mandats sont signés numériquement et cryptés sur le serveur EDI. Les messages sont téléchargés à partir du serveur EDI vers le serveur FTP à l'UPU. Dans le cas des organisations utilisant une configuration VPN client, le logiciel VPN est hébergé sur le serveur EDI. Le serveur EDI communique avec le serveur FTP à l'UPU au moyen d'un tunnel VPN, d'un VPN client ou d'une connexion SFTP.



Pare-feu

Un pare-feu est un dispositif de sécurité qui contrôle et filtre le trafic sur un réseau. Les pare-feu acceptent ou rejettent le trafic sur la base de certains critères, tels que l'adresse IP source, le port source, l'adresse IP de destination, le protocole source ou le nom de domaine de la source (dans ce cas, « source » signifie toujours l'origine du contact). Des paramètres définis par l'utilisateur déterminent quels sont les protocoles d'une source donnée, tels que l'Internet, permettant d'accéder à une destination particulière, comme un poste de travail sur votre réseau. Par exemple, un pare-feu configuré de manière courante rejette tous les protocoles dont la source est l'Internet et dont la destination est l'ordinateur d'un utilisateur, mais il autorise les protocoles HTTP et FTP dont la source est le poste de travail et la destination l'Internet.

Votre réseau doit comporter au moins un pare-feu. La configuration la plus simple est celle selon laquelle tous les utilisateurs d'IFS au sein de l'organisation sont reliés à un réseau local. Les organisations possèdent souvent des réseaux grande distance ou des sites séparés géographiquement mais reliés par des lignes dédiées ou louées. Si l'organisation de votre entreprise comprend des réseaux locaux ou des réseaux grande distance multiples, vous aurez besoin d'un pare-feu à chaque point auquel le trafic entre et sort du réseau.

La manière de mettre en place un pare-feu dépend du type de pare-feu que vous utilisez et de l'objectif particulier de chaque pare-feu. Cette opération, qui peut être régie par des dispositions statutaires ou une réglementation nationale, relève en général de la responsabilité de l'administrateur réseau.

Secure File Transfer Protocol (protocole de transfert de fichiers sécurisé)

Le protocole de transfert de fichiers sécurisé (Secure File Transfer Protocol – SFTP) est une version sécurisée du protocole de transfert de fichiers (File Transfer Protocol – FTP) qui facilite l'accès aux données et leur transfert au moyen d'un flux de données Secure Shell (SSH). Celui-ci fait partie du protocole SSH. Ce processus est également dénommé protocole de transfert de fichiers SSH (**SSH File Transfer Protocol**).

Réseaux privés virtuels

Un réseau privé virtuel (Virtual Private Network – VPN) est un réseau de communication privé utilisé pour communiquer de manière confidentielle via un réseau accessible au public. Un VPN est nécessaire pour toutes les configurations d'IFS. Chaque client doit disposer d'un compte VPN auprès de l'UPU. Pour des raisons de sécurité, ce compte peut être contrôlé et désactivé, en cas de besoin. Seul le trafic VPN est admis par le serveur FTP sur le réseau IFS. Deux configurations VPN sont possibles : Client VPN et tunnel VPN.

Dans le premier cas, le logiciel VPN est installé sur le serveur EDI du client. Dans cette configuration, les données cryptées concernant les mandats vont directement du serveur EDI au pare-feu de l'UPU, en passant par le pare-feu du client. Votre pare-feu doit être configuré de manière à permettre le trafic de données cryptées.

Cette configuration peut ne pas convenir à toutes les organisations, car elle suppose la transmission de données cryptées sur votre réseau (dans les deux sens) entre le serveur EDI et le pare-feu. Il est

possible de voir les paquets de données cryptées sur votre réseau, mais leur contenu ne peut pas être contrôlé.

Dans la deuxième configuration, celle du tunnel VPN, le logiciel VPN est installé sur le pare-feu de votre entreprise. Le tunnel VPN est une configuration de pare-feu à pare-feu. A l'extrémité de la connexion se trouve toujours un autre pare-feu. Dans ce cas, il s'agit du pare-feu de l'UPU. Le tunnel VPN permet aux données cryptées de passez à travers le pare-feu.

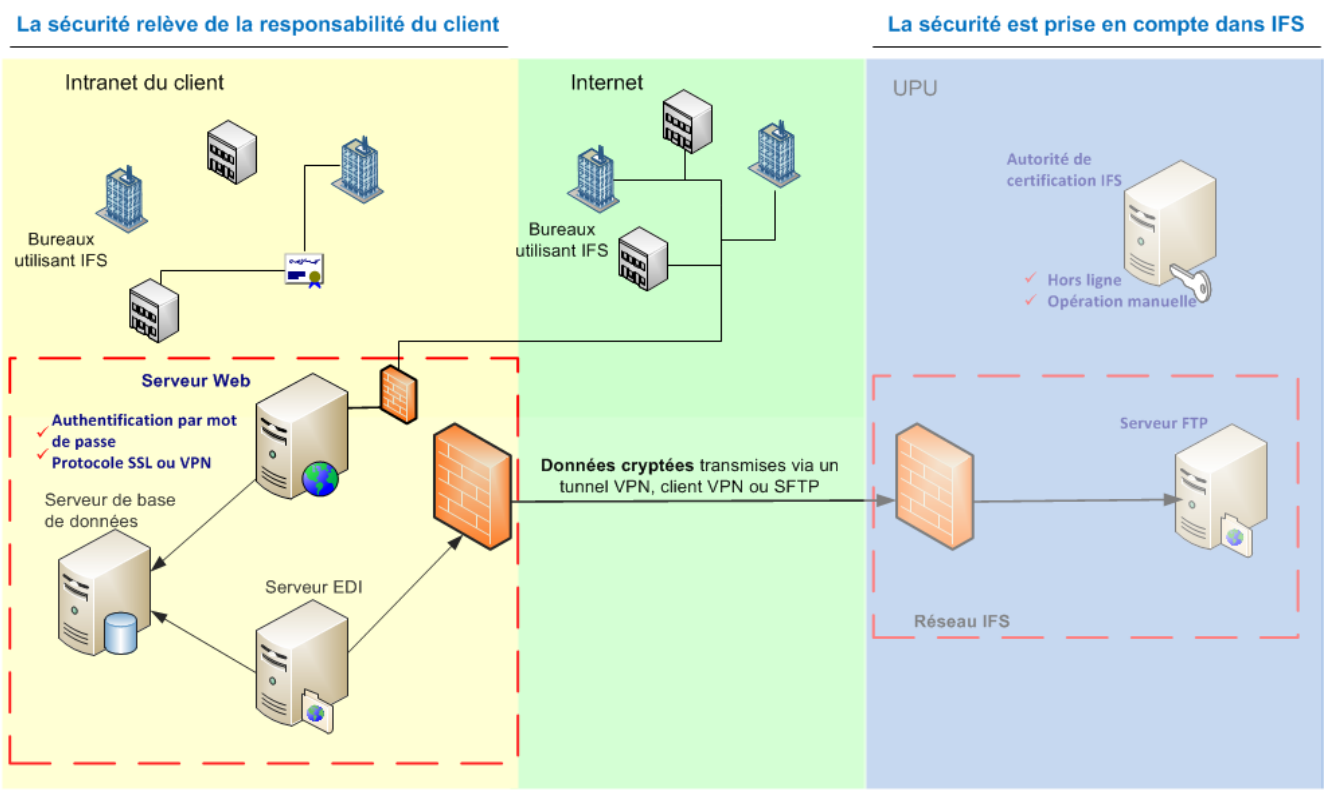
Le VPN est conçu pour crypter davantage les messages relatifs aux mandats, en plus du cryptage déjà effectué par IFS. Ainsi, les données sensibles sont cryptées deux fois lors de leur transmission via l'Internet. Le cryptage VPN est retiré par le VPN à l'arrivée. (Seul le pays partenaire peut décrypter, au moyen de sa clé privée, les données sensibles partiellement cryptées concernant les mandats. Veuillez vous reporter à la section « Cryptage à clé publique et privée » en page 7.)

Pour mettre en place un VPN, vous devez d'abord décider si vous allez utiliser une configuration de type VPN client ou un tunnel VPN. La version client du logiciel VPN utilisée par l'UPU – VPN-1 de Check Point Software Technologies Ltd. – est disponible gratuitement à l'adresse www.checkpoint.com ou auprès du Centre de technologies postales.

Sécurité sur le serveur Web

Dans l'organisation du client, les utilisateurs accèdent à IFS au moyen d'un navigateur Web, tel qu'Internet Explorer de Microsoft. Dans l'organisation du client, les utilisateurs accèdent à l'application Web d'IFS au moyen d'un navigateur, tel qu'Internet Explorer de Microsoft. Les utilisateurs d'appareils mobiles accèdent aux services WEB API d'IFS ouverts à tous sur le même serveur. Il peut aussi être vulnérable aux attaques lancées depuis l'extérieur en l'absence de mesures de protection adéquates, telles que l'installation de pare-feu.

Le mode de sécurisation de votre application Web dépend de l'infrastructure informatique de votre organisation. Si tous les utilisateurs potentiels du système font partie d'un intranet suffisamment protégé, l'UPU recommande une configuration utilisant le protocole SSL; quatre configurations sont envisageables. Toutefois, si des postes de travail client doivent accéder à l'application Web depuis l'extérieur de votre intranet – autrement dit, via l'Internet – cet accès devrait s'effectuer au moyen d'un VPN sur un pare-feu. Des explications plus détaillées concernant ces deux méthodes sont fournies plus loin dans la présente section.



Authentification par mot de passe

Comme c'est le cas pour de nombreuses applications, les utilisateurs doivent saisir un nom et un mot de passe pour se connecter à IFS. En outre, si les utilisateurs accèdent à l'application Web au moyen d'un VPN, chaque utilisateur devra aussi saisir un nom et un mot de passe pour se connecter au VPN client.

Tous les utilisateurs d'IFS dans votre organisation doivent être définis dans IFS. Les utilisateurs doivent aussi être affectés à un ou plusieurs groupes d'utilisateurs IFS. Les utilisateurs ne peuvent accéder qu'aux fonctions associées au groupe d'utilisateurs auquel ils sont affectés. Un mot de passe constitue la première défense contre les accès non autorisés, mais d'autres mesures de protection sont nécessaires car les mots de passe peuvent être volés ou devinés.

Dans l'application Web IFS, un message informe les utilisateurs de la date et de l'heure de leur dernière connexion et/ou leur indique s'il y a eu de vaines tentatives de connexion au moyen de leur nom d'utilisateur depuis leur dernière connexion. Si une atteinte à la sécurité du mécanisme d'authentification par mot de passe est soupçonnée, les utilisateurs devraient demander immédiatement à leur administrateur système IFS d'enquêter sur l'incident.

Les groupes d'utilisateurs sont définis dans l'application de la console de gestion IFS. L'identificateur et le mot de passe de chaque utilisateur sont définis à partir d'une fenêtre dans l'application client d'IFS. Seuls les administrateurs système IFS ont accès à ces fonctions.

Si votre configuration utilise un pare-feu avec un VPN, vous devez définir les identificateurs et mots de passe des utilisateurs au moyen du logiciel VPN dans votre pare-feu.

Quatre niveaux de sécurité basés sur le protocole SSL

La configuration de la sécurité correspondant le mieux à vos besoins dépend de plusieurs facteurs, tels que la taille et l'infrastructure de votre réseau, la configuration des postes de travail utilisant IFS, et les règlements statutaires ou nationaux. Il incombe à chaque client de veiller à la mise en place des mesures de sécurité nécessaires.

A l'instar de la plupart des applications fonctionnant au moyen d'un navigateur Web, IFS utilise HTTP, un protocole que les utilisateurs du Web connaissent bien. Le protocole HTTP a été conçu pour permettre une lecture aisée du contenu des informations transmises, mais il n'est pas protégé. En vue de la transmission sécurisée des données sensibles, le serveur Web hébergeant IFS doit utiliser le protocole SSL. La combinaison des protocoles HTTP et SSL est connue sous le nom de HTTPS. SSL permet de crypter les données et contribue à la réalisation des objectifs de sécurité en matière d'intégrité, de confidentialité et d'authentification.

L'application IFS fonctionne sous IIS (Internet Information Services) sous Windows, qui prend en charge le protocole SSL. Ce dernier utilise des certificats numériques, dont la conception est similaire à celle des certificats utilisés dans IFS. Le serveur – dans ce cas le serveur Web – présente un certificat numérique qui doit être vérifié par le navigateur. Celui-ci n'accepte le certificat que s'il est émis par une autorité de certification figurant dans le répertoire des autorités de certification de confiance sur la machine locale. Le navigateur vérifie en outre si le nom de domaine du site Web correspond au nom de domaine indiqué sur le certificat. La non-concordance de ces noms indique une éventuelle atteinte à la sécurité. La demande peut provenir, par exemple, d'un faux serveur vers lequel un pirate informatique tente de détourner le trafic.

IFS peut prendre en charge quatre niveaux de sécurité établis au moyen du protocole SSL :

- Authentification SSL unidirectionnelle
- Authentification SSL unidirectionnelle et restrictions concernant les adresses IP
- Authentification SSL bidirectionnelle
- Authentification SSL bidirectionnelle et cartes à puce ou clés USB

Chaque niveau de sécurité offre un degré de protection supplémentaire.

Authentification SSL unidirectionnelle

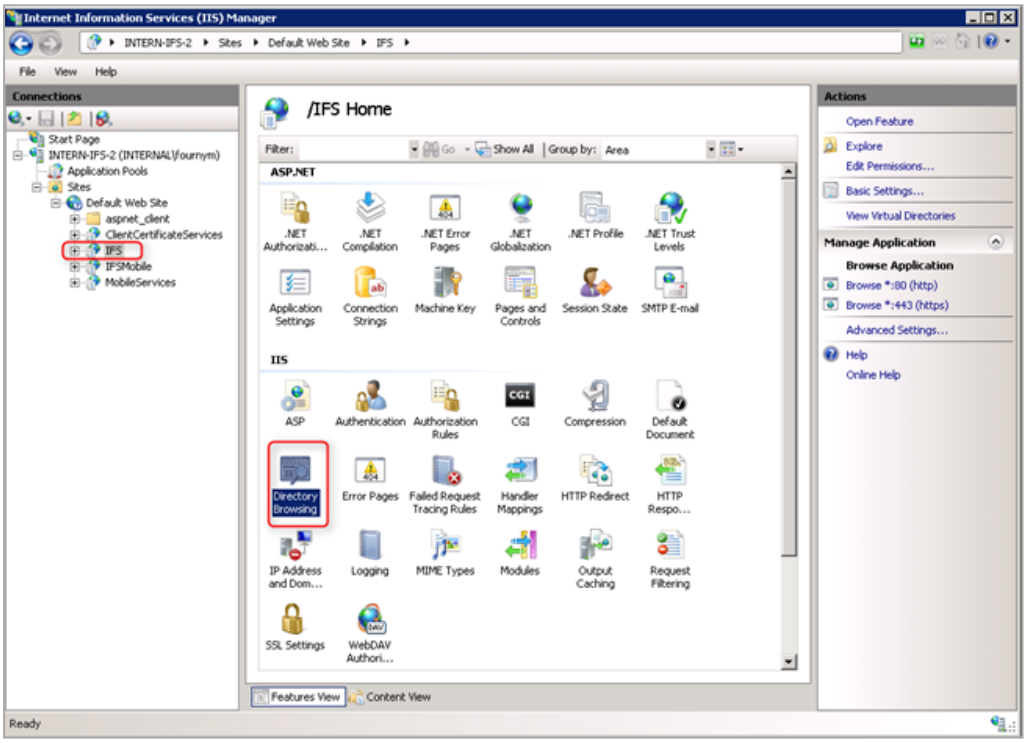
Avec l'authentification SSL unidirectionnelle, les postes de travail n'ont qu'à faire confiance au serveur. L'authentification SSL unidirectionnelle correspond au niveau de sécurité minimal requis pour le serveur Web avec IFS. Vous pouvez configurer IFS pour qu'il passe par SSL en obtenant un certificat d'une autorité de certification racine. Ce type de certificat est inclus par défaut dans les navigateurs Web les plus courants (Internet Explorer, Firefox, Safari, Opera, Chrome).

Sur le serveur Web IIS de Microsoft, vous pouvez faire une demande de certificat SSL et installer le certificat au moyen de l'assistant pour la création de certificats de serveur Web, accessible à partir de la section « propriétés » sur votre site Web IFS.

Authentification SSL unidirectionnelle et restrictions concernant les adresses IP

L'une des solutions pour renforcer la sécurité consiste à utiliser des adresses IP statiques sur les postes de travail et à réserver l'accès à l'application Web IFS à ces seules adresses IP. Les adresses IP statiques ne sont pas adaptées à toutes les situations, car elles peuvent être vulnérables aux attaques de pirates informatiques qui manipulent les données pour faire croire qu'elles proviennent d'une machine différente.

Vous pouvez définir les adresses IP ayant accès à l'application Web IFS au moyen de la console de gestion IIS. Ouvrez la pages Propriétés de l'application IFS, sur le site Web par défaut. Cliquez sur l'onglet **Directory Security**, puis sur le bouton **Edit** dans la section sur les restrictions relatives aux adresses IP et aux noms de domaine.



Authentification SSL bidirectionnelle

Dans cette configuration, l'authentification SSL s'effectue à la fois sur le serveur et sur les postes de travail. Les clients (les postes de travail utilisant IFS) présentent aussi des certificats qui doivent être acceptés par le serveur. Le serveur n'accepte que les demandes émanant de postes de travail dont les certificats ont été émis par une autorité de certification de confiance.

L'authentification SSL bidirectionnelle renforce la sécurité, mais elle entraîne aussi une forte augmentation du temps système, puisque des certificats sont alors requis pour chaque poste de travail qui se connecte à l'application Web IFS.

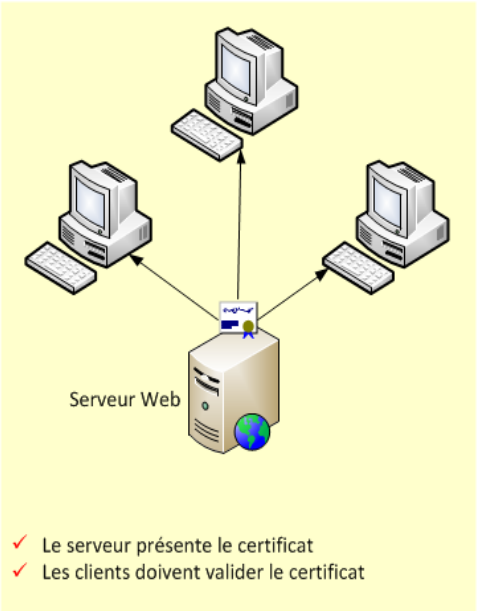
Pour de plus amples informations sur les certificats, veuillez soit contacter une société privée (Verisign), soit utiliser un organisme d'authentification gratuit (https://letsencrypt.org/).

Authentification SSL bidirectionnelle et cartes à puce ou clés USB

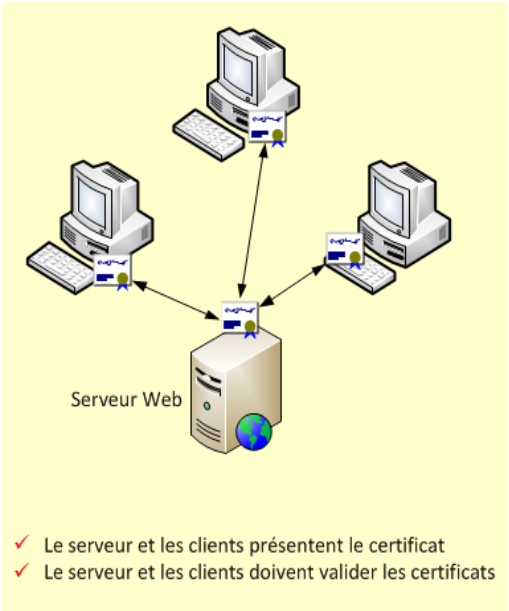
Une autre solution pour renforcer encore davantage la sécurité consiste stocker les certificats des clients sur des cartes à puce ou des clés USB. Ces éléments sont portables et protégés par un mot de

passe. Le certificat SSL est stocké sur la carte à puce ou la clé USB. Pour obtenir l'autorisation d'accéder au site Web, l'utilisateur doit connecter la carte à puce ou la clé USB et saisir son mot de passe personnel.

Authentification SSL unidirectionnelle



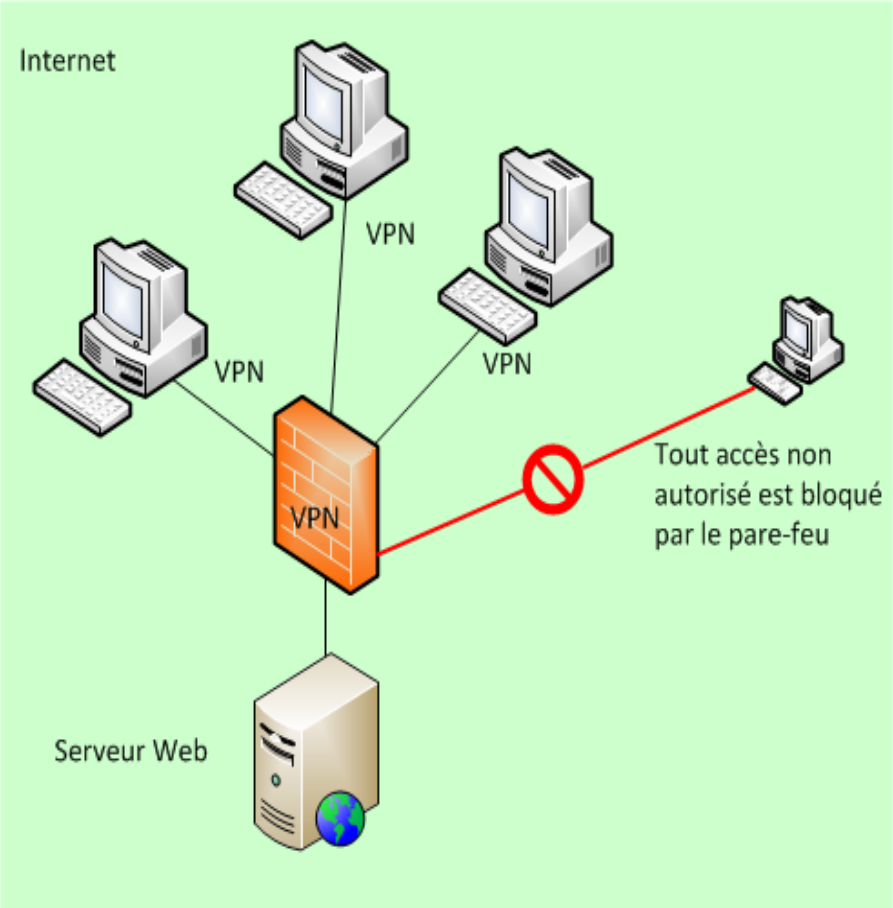
Authentification SSL bidirectionnelle



Pour de plus amples informations sur les cartes à puce et les clés USB, veuillez prendre contact avec un fournisseur de ce type de matériel. Vous pouvez par exemple vous adresser aux sociétés SafeNet ou Aladdin.

Utilisation d'un VPN pour protéger l'application Web

Si certains de vos utilisateurs travaillant dans des bureaux distants doivent accéder à l'application Web IFS via l'Internet, l'UPU recommande une approche différente. Si certains de vos utilisateurs ne sont pas protégés par un pare-feu, il est recommandé de faire passer le trafic provenant de l'Internet à travers un pare-feu avec un VPN.



Dans cette configuration, il n'y pas d'authentification SSL. L'accès à l'application Web IFS est limité aux utilisateurs VPN autorisés. A chaque poste de travail correspond un compte d'utilisateur et un mot de passe qui permettent de se connecter à l'application Web. Le trafic entre les postes de travail et le serveur est crypté.

Si le composant Services Web IFS est également utilisé avec une adresse publique afin d'offrir un accès aux appareils mobiles, vous pouvez utiliser un autre site que le site par défaut pour le composant Web IFS. Vous pouvez par ailleurs configurer différents ports et différents sites pour chaque composant afin d'utiliser le VPN exclusivement pour l'application Web IFS.

Pour obtenir des informations complémentaires au sujet du VPN, vérifiez si votre routeur/pare-feu offre ce service ou utilisez un service de VPN gratuit, tel que OpenVPN (https://openvpn.net/).

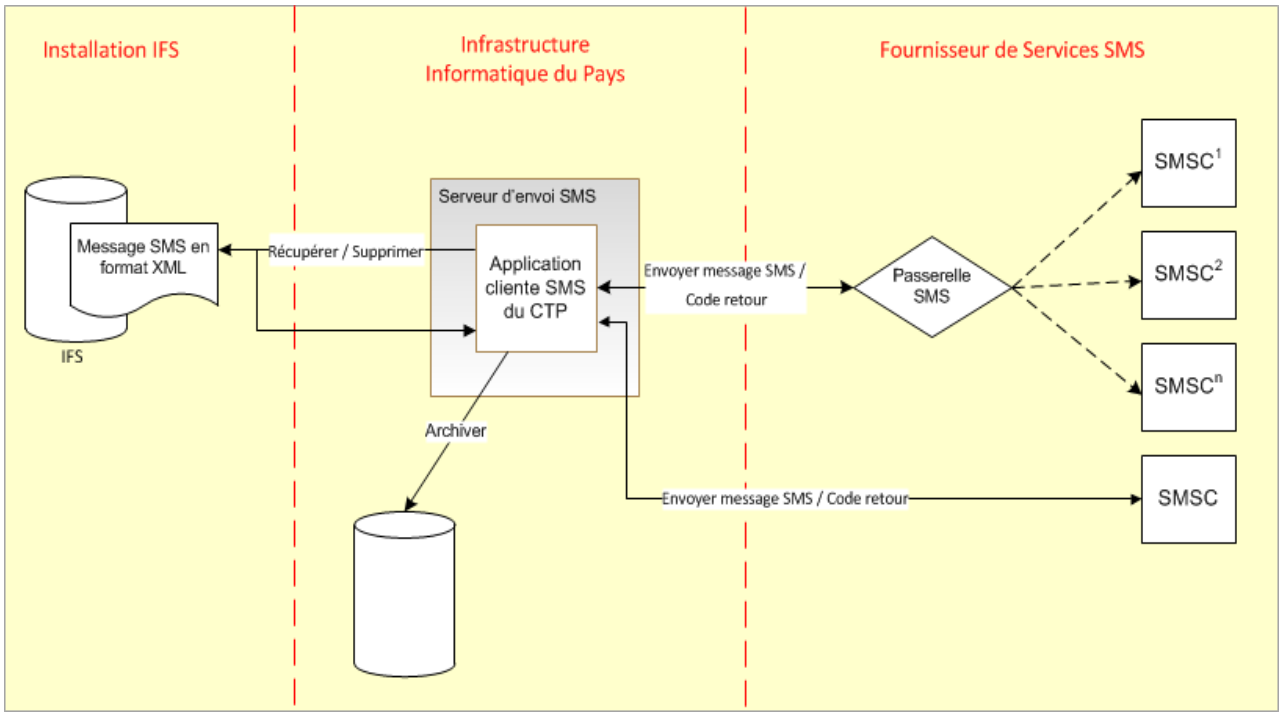
Utilisation de l'authentification Windows

Une dernière possibilité consiste à restreindre l'accès à l'application Web IFS à un ensemble limité d'utilisateurs Windows au moyen du module de gestion de l'authentification et des autorisations de la console de gestion IIS. Cette configuration est fortement recommandée lorsque les utilisateurs de chaque bureau sont déjà configurés sur le réseau avec un compte Active Directory.

Pour obtenir des informations complémentaires sur la gestion de l'authentification et des autorisations, veuillez consulter la documentation IIS dans la bibliothèque TechNet de Microsoft (https://technet.microsoft.com).

Sécurisation du lien entre l'installation d'IFS et l'application de passerelle SMS locale

Le schéma ci-après illustre la liaison entre le serveur Web IFS et un fournisseur de services SMS par le biais d'une passerelle SMS.



Les récépissés par SMS sont générés sur le serveur Web IFS, au sein de la structure de fichier suivante :

SMS

SMS\Récépissé

SMS\Récépissé\International

SMS\Récépissé\International\Emis

SMS\Récépissé\International\Payé

SMS\Récépissé\International\Remboursé

SMS\Récépissé\National

SMS\Récépissé\National\Emis

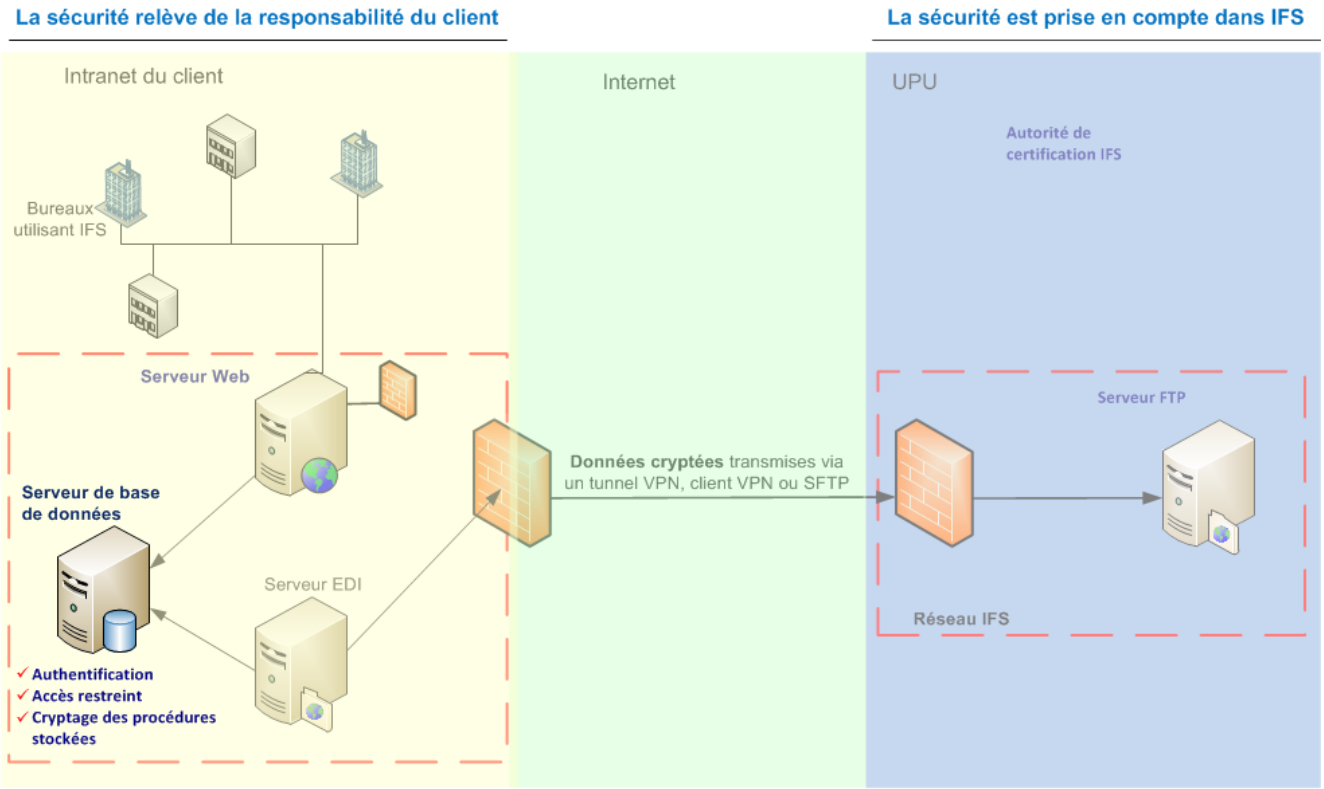
SMS\Récépissé\National\Payé

SMS\Récépissé\National\Remboursé

Il incombe au client de restreindre l'accès à ces dossiers aux utilisateurs pertinents. Il s'agit habituellement de l'utilisateur IFSUser et de l'utilisateur du serveur d'envoi de SMS fourni par le client, comme indiqué sur le schéma ci-dessus.

Indépendamment des mécanismes intégrés pour la protection des données mentionnés dans la section précédente, le client doit assumer une responsabilité supplémentaire en ce qui concerne le stockage de données relatives aux mandats sur le serveur de la base de données IFS dans une base de données SQL. La base de données de production IFS renferme les données concernant tous les mandats en cours ainsi que les données de suivi y relatives. La plupart des organisations ont aussi une base de données d'archives contenant des informations sur les transactions effectuées.

Il faudrait protéger davantage le serveur de la base de données au moyen d'un mécanisme d'identification et en limitant l'accès à la base de données aux procédures stockées dans la base de données IFS. L'accès à la base de données à des fins administratives devrait normalement être limité aux administrateurs système IFS.



L'application Microsoft SQL Server doit être installée sur le serveur qui hébergera la le serveur de la base de données. La solution permettant d'obtenir les meilleurs résultats consiste à utiliser ce serveur exclusivement pour l'hébergement de la base de données IFS, mais cela n'est pas obligatoire. La machine hébergeant la base de données peut aussi servir de serveur EDI ou de serveur Web.

Authentification

Le service IIS sur le serveur Web utilise un compte d'utilisateur spécifique pour accéder à la base de données IFS. Il existe deux moyens d'authentification : l'authentification SQL Server et l'authentification Windows. La méthode d'authentification varie selon que le serveur de la base de données et le serveur Web sont sur la même machine ou sur des machines distinctes. L'authentification Windows ne peut être utilisée que si le serveur de la base de données et le serveur

Web se trouvent sur la même machine ou constituent le même domaine. L'authentification Windows utilise un identificateur d'utilisateur et un mot de passe définis dans Windows. Il s'agit d'un identificateur spécifique utilisé uniquement par IIS pour accéder à la base de données.

Pour l'authentification SQL, l'identificateur de l'utilisateur et le mot de passe utilisés pour la connexion à la base de données sont définis dans SQL. L'identificateur et le mot de passe peuvent être créés lors de l'installation d'IFS ou définis dans SQL Enterprise Manager avant l'installation.

Il est important de comprendre que ces codes de connexion ne sont pas les mêmes que ceux qu'emploient les utilisateurs pour accéder au système IFS. Il s'agit de codes spéciaux utilisés uniquement par le serveur Web pour accéder à la base de données.

L'application SQL Server non seulement gère les accès au niveau de la base de données, mais effectue aussi un contrôle en fonction des rôles pour autoriser ou refuser l'accès à des fonctions particulières. Un rôle représente un groupe, semblable à un groupe d'utilisateurs, auquel des codes d'accès personnels/utilisateurs peuvent être ajoutés. Au cours de son installation, IFS crée un rôle dénommé « IFSUsers » (utilisateurs IFS) auquel il attribue automatiquement le code d'accès Windows ou SQL que vous avez créé. La seule tâche que ce rôle permet d'accomplir est l'exécution des procédures IFS stockées.

Procédures stockées

Des procédures stockées sont des programmes précompilés qui s'exécutent sur une base de données. IFS utilise des centaines de procédures stockées. Ces procédures stockées sont cryptées. Les procédures stockées servent généralement à saisir des processus opérationnels et à manipuler des données. Dans IFS, par exemple, de nombreuses procédures stockées inscrivent des informations dans les tableaux IFS. Les tableaux dans la base de données ne peuvent être modifiés qu'au moyen de la procédure stockée. Aucune fonction, telle que la modification d'un tableau comportant des données relatives à des mandats, ne peut être exécutée manuellement à moins qu'un utilisateur ne soit assigné à un rôle permettant de le faire. Le seul qui puisse créer un tel rôle est l'administrateur système.

Sécurité au niveau des clients Web

La plupart des navigateurs sont dotés d'une fonction de navigation multi-onglets. A moins que votre entreprise n'ait besoin de cette fonction pour d'autres applications utilisant le même navigateur, nous recommandons de la désactiver. En effet, un récent code d'exploitation dénommé Cross Site Request Forgery (CSRF) (Injection de requête illégitime par rebond) pourrait exploiter cette fonction à des fins malveillantes.

L'application Web IFS dispose déjà d'une protection intégrée contre ce type de vulnérabilité, mais les attaques évoluent sans cesse. C'est pourquoi nous recommandons de désactiver la navigation multi-onglets.

Pour désactiver la navigation multi-onglets sur Internet Explorer 8, sélectionnez **Outils > Options Internet > Général > Onglets > Paramètres** et désactivez la case à cocher **Activer la navigation par onglets**.

Mises à jour de sécurité

Des mises à jour de sécurité et des corrections de bogues et de programmes sont diffusées régulièrement par les fournisseurs d'applications logicielles. Ces corrections résultent souvent de la découverte de failles dans les logiciels ou d'attaques au moyen de programmes malveillants, tels que les virus.

Les mises à jour et corrections de Microsoft Windows devraient être exécutées régulièrement sur toutes machines IFS et les clients Web IFS devraient utiliser la dernière version du navigateur de votre choix.

Il se peut que vous exécutiez, sur les mêmes machines ou sur le même réseau que ceux utilisés pour IFS, des applications, telles que Java, Quicktime, RealPlayer et Adobe Reader, susceptibles d'être attaquées par des logiciels malveillants. Ces applications devraient aussi être mises à jour régulièrement ou désinstallées si elles ne sont pas utilisées.

Antivirus et protection contre les logiciels malveillants

Les logiciels malveillants pouvant affecter IFS comprennent notamment : les logiciels espions (enregistreurs de frappe), les vers, les chevaux de Troie, les kits racine et les virus informatiques. Il est vital que vous protégiez vos systèmes informatiques au moyen d'un antivirus. Parmi les principaux fournisseurs de logiciels antivirus figurent : Norton/Symantec, McAfee, Panda Security, Avira et Kaspersky Lab.

Comment obtenir de plus amples informations

Documents et sites Web

Documents disponibles auprès du Centre de technologies postales :

- *Guide d'installation IFS*
- *Working architectures for VPN security*

Sites Web recommandés :

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

Adresse IP

Numéro identifiant chaque expéditeur ou destinataire d'informations transmises par lots via l'Internet.

AES Advanced Encryption Standard

La norme Advanced Encryption Standard (norme de cryptage avancée) est un algorithme de cryptage symétrique qui a été adopté par l'US National Institute of Standards (Institut américain de normalisation) en 2001. Les algorithmes de cryptage AES ont fait l'objet d'analyses approfondies et sont actuellement employés partout dans le monde.

Authentification

Processus de vérification de l'identité numérique de l'expéditeur d'une communication visant à garantir que les données proviennent bien de la source indiquée.

Autorité de certification - AC

Organisation qui fournit et gère des éléments d'authentification et des clés publiques pour le cryptage des messages. Une AC peut être un service public chargé de fournir des certificats payants. Une AC peut être un service public chargé de fournir des certificats payants. Il peut aussi s'agir d'un service privé mis en place par une organisation pour gérer ses propres certificats.

Certificat numérique

Elément d'authentification électronique utilisé pour vérifier qu'un site Web est bien le site indiqué. Les certificats sont émis par des organisations dénommées autorités de certification. Leur tâche consiste à vérifier que le certificat appartient à l'organisation dont le nom y est indiqué.

Cheval de Troie

Logiciel malveillant qui semble effectuer une tâche souhaitée par l'utilisateur, mais qui, en réalité, facilite l'accès non autorisé au système informatique de ce dernier.

Clé privée

Clé de cryptage/décryptage que la ou les parties échangeant des messages secret sont les seules à connaître.

Clé publique

Clé de cryptage qui, combinée avec une clé privée dérivée de la clé publique, peut être utilisée pour crypter efficacement des messages et des signatures numériques.

Code d'authentification des messages basé sur le hachage

Mécanisme d'authentification de messages utilisant des fonctions de hachage. Il s'agit d'une construction spécifique pour le calcul des signatures comprenant une fonction de hachage cryptographique combinée avec une clé secrète.

Confidentialité

Assurance que les informations sont accessibles uniquement à ceux qui sont autorisés à y accéder.

Cross Site Request Forgery (CSRF) (Injection de requête illégitime par rebond)

Infiltration malveillante d'un site Web par laquelle des ordres non autorisés sont transmis par un utilisateur de confiance du site. Les attaques de type CSRF les plus courantes proviennent de scripts exécutés dans des onglets parallèles du navigateur d'un utilisateur, dans le cadre d'une session que l'utilisateur a ouverte dans un onglet distinct.

Disponibilité

Processus visant à garantir que les données sont protégées contre la destruction et que les données, le système ou le service sont disponibles.

EDI

Transfert de données entre différentes parties via à un réseau ou l'Internet.

Enregistreur de frappe

Logiciel qui enregistre les touches utilisées sur un clavier, généralement d'une manière cachée, de sorte que la personne utilisant le clavier n'est pas consciente que ses actions sont surveillées. Dans le cas d'un client Web IFS, les données d'identification d'un utilisateur (c.-à-d. son nom d'utilisateur et son mot de passe) pourraient être volées au moyen de ce mécanisme.

FTP

File Transfer Protocol (protocole de transfert de fichiers). Il s'agit d'un protocole Internet standard utilisé pour échanger des fichiers entre ordinateurs sur l'Internet. Le protocole FTP est généralement utilisé pour télécharger des programmes et d'autres fichiers vers un ordinateur à partir d'autres serveurs.

Hardware Security Module (HSM) (Module matériel de sécurité)

Un HSM est un système matériel cryptographique conçu pour générer, stocker et protéger les clés cryptographiques.

HMAC

Mécanisme d'authentification de messages utilisant des fonctions de hachage. Il s'agit d'une construction spécifique pour le calcul des signatures comprenant une fonction de hachage cryptographique combinée avec une clé secrète.

Intégrité

Assurance que seules les personnes autorisées peuvent accéder à certaines informations ou les modifier.

Internet

Système mondial de réseaux informatiques. Il s'agit d'un réseau de réseaux sur lequel les utilisateurs d'un quelconque ordinateur peuvent, s'ils y sont autorisés, obtenir des informations de n'importe quel autre ordinateur (et parfois communiquer directement avec les utilisateurs d'autres ordinateurs).

Internet Information Services (Microsoft IIS)

Application commerciale de serveur Web sur laquelle l'application Web IFS est hébergée.

Intranet

Réseau privé interne d'une entreprise. Il peut être constitué de nombreux réseaux locaux interconnectés et aussi utiliser des lignes louées sur le réseau grande distance. Un intranet comprend généralement des connections vers l'Internet établies par l'intermédiaire de portails.

Kit racine

Système logiciel comprenant un ou plusieurs programmes conçus pour dissimuler le fait que l'intégrité d'un système a été compromise. Un intrus peut utiliser un kit racine pour remplacer des programmes exécutables vitaux.

Logiciel espion

Type de logiciel malveillant installé sur des ordinateurs pour collecter des informations sur leurs utilisateurs à l'insu de ces derniers. Les enregistreurs de frappe font partie de la catégorie des logiciels espions.

Logiciel malveillant

Logiciel conçu pour perpétrer un acte malveillant en infiltrant un système informatique sans le consentement éclairé de son propriétaire. Il s'agit d'un terme générique recouvrant une variété de logiciels ou de codes programmes hostiles, intrusifs ou agaçants.

Non-répudiation

Assurance qu'un expéditeur de données ne peut pas nier avoir envoyé celles-ci et que le destinataire ne peut pas nier les avoir reçues.

Pare-feu

Système ou configuration logicielle protégeant les ressources d'un réseau privé des utilisateurs d'autres réseaux. Un pare-feu se présente généralement comme une configuration sur un serveur, mais il peut aussi être placé au niveau d'un routeur. Il existe aussi des pare-feu matériels.

Protocole

Série particulière de règles employée par des ordinateurs pour communiquer entre eux sur un réseau.

Protocole SSL

Secure Sockets Layer, en anglais. Protocole couramment utilisé pour gérer la sécurité des messages transmis via Internet.

Serveur de base de données

Machine sur l'intranet d'un client servant à héberger la base de données IFS.

Serveur EDI

Machine sur l'intranet d'un client qui crypte les messages EDI et les envoie vers le serveur FTP de l'UPU.

Serveur FTP

Serveur sur le réseau IFS qui reçoit les messages EDI cryptés renfermant les données concernant les mandats.

Serveur Web

Machine sur laquelle l'application IFS est installée au sein de votre organisation.

SFTP

Le protocole de transfert de fichiers sécurisé (Secure File Transfer Protocol – SFTP) est une version sécurisée du protocole de transfert de fichiers (File Transfer Protocol – FTP) qui facilite l'accès aux données et leur transfert au moyen d'un flux de données Secure Shell (SSH). Celui-ci fait partie du protocole SSH. Ce processus est également dénommé protocole de transfert de fichiers SSH (**SSH File Transfer Protocol**).

SSH

Le protocole SSH utilise la cryptographie à clé publique pour authentifier un ordinateur distant et lui permettre d'authentifier l'utilisateur, le cas échéant. Le protocole SSH peut être utilisé de différentes manières. Il est par exemple possible d'utiliser des paires de clés publiques-privées générées de façon automatique pour crypter simplement une connexion de réseau, puis d'utiliser l'authentification par mot de passe pour se connecter.

Il est également possible d'utiliser une paire de clés publique-privée générées manuellement pour procéder à l'authentification, ce qui permet aux utilisateurs ou aux programmes de se connecter sans avoir à spécifier un mot de passe. Dans ce cas, tout le monde peut produire une paire correspondante de clés différentes (publique et privée). La clé publique est placée sur l'ensemble des ordinateurs qui doivent autoriser l'accès au propriétaire de la clé privée correspondante (le propriétaire préserve la confidentialité de la clé privée). Même si l'authentification repose sur la clé privée, la clé en elle-même n'est jamais transférée sur le réseau au cours du processus d'authentification. Le protocole SSH vérifie simplement si la personne offrant la clé publique détient également la clé privée correspondante. Dans toutes les versions du protocole SSH, il est important de vérifier les clés publiques inconnues, c'est-à-dire d'associer les clés publiques à des identités avant de les accepter en tant que clés valides. Le fait d'accepter la clé publique d'un pirate sans validation l'autorisera en tant qu'utilisateur valide.

Ver

Programme informatique autoreproductible. Le ver utilise un réseau pour envoyer des copies de lui-même à d'autres ordinateurs reliés au réseau, et il peut le faire en l'absence de toute intervention d'un utilisateur. Si un ver infecte l'un de vos clients IFS, il pourrait se répandre à travers votre réseau à l'ensemble de vos clients, voire infecter vos serveurs.

Virus

Programme informatique pouvant se dupliquer et infecter un ordinateur. Les virus informatiques classiques sont capables de détruire intégralement un système d'exploitation ou un système de fichiers.

VPN

Réseau utilisant une infrastructure de télécommunication publique, comme l'Internet, pour fournir à des bureaux distants ou à des utilisateurs individuels un accès sécurisé au réseau de leur organisation.

XML

Extensible Markup Language, en anglais. XML est une série de règles flexibles permettant d'encoder des documents électroniquement. XML permet de créer des documents dans un format commun, de sorte que les informations puissent être partagées sur le Web, sur des intranets ou ailleurs.