



NAXFER

WHITE PAPER

Transfert de données Poste à poste sécurisé
Comprendre les bénéfices du transfert poste à poste hautement sécurisé.

Julien Conan

J&S CONCEPT

Fiche Produit

© 2009 Ce document est propriété de J&S CONCEPT.

Sommaire

Introduction	3
Comment innover ?	4
NAXFER, facile, sécurisé, fiable	6
Fonctionnalités et détails techniques	8
Présentation	8
Authentification	9
Protocole réseau et confidentialité	9
Stockage des données sur le poste réception	10
Spécifications techniques	10

Introduction

De nos jours, les entreprises travaillent avec diverses agences, clients et fournisseurs sur le territoire international. Ces entités échangent quotidiennement des données que ce soit sous forme de fichiers lourds ou sous forme de supports numériques (CD, DVD, clé USB etc..). Ces échanges sont essentiels au bon fonctionnement du groupe et des délais de production. Il a été constaté que, l'homogénéité, la confidentialité, la conformité et la rapidité des données échangées sont primordiales.

Actuellement, les sociétés ne disposent pas de système homogène d'échange entre leurs diverses entités. Les moyens d'échange utilisés à ce jour sont :

- **Les emails:** Simples d'utilisation, ils ne sont adaptés que pour des fichiers de petite taille et n'offrent en aucun cas, une garantie de conformité. Par ailleurs, ils sont inadaptés aux éléments nécessitant de la confidentialité et ne peuvent transmettre des fichiers de plus de 5 à 10 Mo Maximum.
- **Les serveurs FTP:** Trop complexes d'utilisation pour les utilisateurs non experts (adresse IP, mot de passe, interfaces ayant trop de menus et d'options etc....) ils nécessitent une gestion permanente de la part des équipes informatiques lorsqu'ils sont hébergés en interne. Cette gestion inclue entre autre, la gestion des permissions des divers comptes, le nettoyage des répertoires, la transmission des mots de passe en cas d'oubli, les créations de comptes utilisateurs etc....

Lorsqu'ils sont hébergés sur des serveurs Internet, ils souffrent de lenteurs et sont parfois indisponibles. Ils nécessitent également un contact fréquent avec les hébergeurs qui prennent en charge la gestion des comptes et des permissions.

Dans tous les cas, le FTP n'offre pas de confidentialité ni de garantie de conformité. Les données transmises sont exposées chez les hébergeurs et libres d'accès pour tout employé y travaillant.

D'autre part, aucune trace du jour et de l'heure ou de l'émetteur n'est conservée de façon fiable lors d'un transfert, ce qui pose un réel problème en cas de contestation ou de conflit dus à des corruptions de fichiers. De telles conditions, ne permettent pas de déterminer précisément les responsabilités.

Enfin, dans le cas de données se trouvant sur des CD ou des DVD, bien que le FTP soit adapté à l'envoi de contenus volumineux, le manque de garanties et la nécessité de générer des images ISO des médias avant l'envoi, rendent la tâche difficile voire impossible pour un non initié (intervention du service technique obligatoire).

- **Les serveurs Web de dépôt et d'échange de fichiers:** Bien que plus simples d'utilisation que le FTP, ils souffrent des mêmes inconvénients et accusent une lenteur supplémentaire due au manque de fiabilité du protocole http et aux débits souvent trop bas des serveurs Web offrant ce genre de services.
- **Les envois par coursier:** Ils restent le moyen privilégié utilisé par les entreprises pour l'envoi des fichiers graphiques et des supports médias.

Malheureusement, les livraisons par coursiers ou autres, sont tributaires des distances géographiques et deviennent particulièrement lentes à l'international. Or les délais de livraisons ont une grande importance dans le domaine de la publicité et de la création graphique par exemple. Ils peuvent rapidement se convertir en un frein à la productivité.

Par ailleurs, ils représentent un coût non négligeable qui, rapporté au nombre d'exemplaires qui transitent annuellement, constituent un coût considérable. Il s'avère que ce coût, frôle parfois le million d'Euros.

Comment innover ?

Afin d'offrir à l'utilisateur final une solution adaptée aux besoins actuels d'échange des données, des innovations devront être introduites. Au minimum, les problématiques ci dessous devront être prises en charge de façon conviviale et intuitive afin d'apporter aux utilisateurs une solution rapide, performante et satisfaisante.

- **Sécuriser l'authentification:** La solution devra fournir une méthode très sécurisée et fiable pour authentifier les utilisateurs. Il est aujourd'hui de notoriété publique que les « login » et mots de passe sont bien trop faible en terme de sécurité. L'authentification forte basée sur les identités numériques (certificats) doublée avec des périphériques de stockage et de verrouillage matériels, tels les dongles USB ou les cartes à puce, sont de très bons candidats.
- **Hétérogénéité des données:** La solution devra permettre aux utilisateurs de se débarrasser de leurs frais de port liés au transfert de données, de CD ou de DVD dans la chaîne de production. En effet, les débits internet élevés disponibles aujourd'hui sont en pleine augmentation. Dans les années à venir, il est évident que le transfert de plusieurs Giga octets à travers internet sera chose réalisable.

- **Eviter les serveurs intermédiaires:** Supprimer les serveurs intermédiaires et de stockage devrait réduire drastiquement la durée des transferts d'un site à l'autre. Une connexion poste à poste fournirait une exploitation optimale du débit entre l'émetteur et le récepteur. Par ailleurs, la corvée de la gestion des espaces de stockage et de leur confidentialité devra être épargnée. Enfin, toutes les coupures de connexion ou les baisses de qualité des lignes devront être prises en charge par la solution.
- **Sécuriser le transfert:** La confidentialité pendant le transfert devra être un aspect obligatoire de la solution. Les plus hauts niveaux d'encryption disponibles devront être utilisés.
- **Optimiser l'automatisation des tâches:** Les logiciels de transfert devront gérer automatiquement des tâches que la recherche des adresses et des réseaux des destinataires, la génération des images ISO des CDs, la signature numérique, l'encryption et le transfert. De plus, des interfaces simples et ergonomiques devront être présentées à l'utilisateur final de façon à lui offrir une expérience d'utilisation agréable et intuitive.
- **Fournir de la fiabilité et de la conformité:** Après chaque transfert, une preuve fiable de la conformité devra être produite et archivée. Elle devra contenir au moins les éléments suivants:
 - Identité de l'émetteur et du récepteur.
 - Date et heure de la transmission.
 - Détails des données transmises (nom, extension, taille).
 - Attestation de conformité des données.
- **Eviter la nécessité d'une installation:** L'installation d'un logiciel devra être évitée tant que possible. Généralement, cette dernière est une contrainte pour l'utilisateur final et la plupart du temps elle requiert des droits d'administrateur que la plupart des utilisateurs n'ont pas. La propagation du logiciel et son acceptabilité dépendront de sa facilité de déploiement. Les technologies basées sur les navigateurs web comme les scripts clients, objets COM ou les technologies Java WebstartWeb semblent être le meilleur choix.

NAXFER, facile, sécurisé, fiable

NAXFER est un logiciel qui tire le meilleur parti des avantages des technologies poste à poste (P2P) modifiées, ne générant plus aucun point d'intrusion, afin d'offrir à l'utilisateur une solution de transfert de contenus lourds ultra sécurisés de façon simple, rapide et intuitive.

Les avantages qu'offre NAXFER à toute entreprise ayant besoin d'échanger régulièrement des médias et des éléments graphiques volumineux ou de simples fichiers, avec ses partenaires filiales ou clients sont nombreux :

- **Sécurité maximale:** NAXFER tire parti des technologies d'authentification forte par certificat X509. Cette particularité permet à NAXFER de garantir l'identité de l'expéditeur et de se prémunir ainsi, des piratages d'identité qui sont de plus en plus répandus.

Les informations concernant l'identité de l'utilisateur ainsi que ses clés privées sont stockées sur une clé USB HASP. Cette clé fabriquée par la société Aladdin, leader dans le monde, des clés cryptographiques, possède une zone cachée protégée qui garantit la sécurité des clés privées en cas de vol de la clé.

- **Transfert automatique des médias:** NAXFER dématérialise automatiquement des CD, DVD, Blu-Ray, HD DVD, avant leur envoi et reconstitution automatique à l'autre bout de la terre, après leur réception. NAXFER ne nécessite l'installation d'aucun logiciel de gravure tel que Nero ou Roxio. Grâce à son partenariat avec la société DROPPIX, NAXFER intègre ses propres bibliothèques de gravure. Ces bibliothèques bénéficient de l'expérience et du savoir faire de la société DROPPIX qui développe les firmwares de robots de gravure industriels depuis de nombreuses années.
- **Envoi poste à poste:** La performance est assurée par une architecture poste à poste, permettant d'éliminer les intermédiaires, les retards et les lenteurs dues à l'utilisation de serveurs web intermédiaires, FTP ou serveurs de mails très souvent limités.
- **Confidentialité:** NAXFER offre également une confidentialité de haut niveau, grâce à l'utilisation de l'algorithme de chiffrement AES avec des clés de 256 bits. Cet algorithme est le plus robuste et le plus performant actuellement sur le marché et bénéficie d'une autorisation de la direction centrale de la sécurité des systèmes d'information (DCSSI).



- **Utilisation conviviale adaptée pour tous:** L'interface du logiciel NAXFER a été conçue pour permettre d'effectuer les opérations d'envoi et de vérification en 3 ou 4 clics. Aucune connaissance informatique n'est nécessaire. L'expéditeur n'a ni besoin de mot de passe, ni de connaître les adresses IP. La recherche et l'importation du destinataire s'effectue grâce à un annuaire Web propriétaire, similaire à celui des pages jaunes. Des notifications par messages visuels signalent automatiquement au destinataire l'arrivée d'un contenu et ce dernier peut suivre la progression de la réception en temps réel.
- **Garantie de conformité et de fiabilité:** Les corruptions de fichiers et les médias non-conformes ne sont plus une inquiétude avec NAXFER. En effet, ce dernier intègre des certificats de conformité infalsifiables basés sur empreintes et signatures numériques. Ces certificats de conformité sont délivrés après chaque transfert et permettent de garantir à tout moment la conformité du contenu, l'horodatage et l'identité de l'expéditeur.
- **Déploiement ultra simplifié:** La technologie propriétaire de NAXFER, « Routeur Virtuel », lui permet de s'intégrer automatiquement avec les équipements réseaux (firewall, proxys etc..). L'envoi et la réception sur le poste ne nécessitent aucune intervention sur les routeurs ou les firewalls et n'impactent pas l'architecture réseau. Enfin, que le poste utilisateur soit sous Microsoft Windows 2000 +, Linux (les grandes distributions connues) ou MAC OS X 10.5+, il pourra faire fonctionner NAXFER.



Fonctionnalités et détails techniques

Présentation

Le logiciel NAXFER se présente sous la forme de 3 interfaces. Il doit être installé sur le poste de l'émetteur uniquement. Le récepteur n'a pas besoin d'installer le logiciel car ce dernier se lancera automatiquement à partir de son navigateur lorsqu'il recevra des données. Cependant, une installation sur le poste du récepteur ouvre des fonctionnalités avancées.

NAXFER se décline en 3 parties:

- **Interface d'envoi:** Elle permet d'envoyer des fichiers, dossiers, Cds, DVDs, Blurays et documents papier. Elle dématérialise l'ensemble des medias automatiquement et gère les coupures de connexion. Cette interface nécessite une installation.
- **Interface de réception:** Elle permet d'extraire les dossiers et fichiers reçus qui sont conservés dans un format crypté et compressé sur le disque et d'imprimer les documents papiers reçus. Dans sa version complète, elle permet également de regraver les CDs,DVDs et Blurays reçus.

Elle se décline donc sous 2 formes :

- Une interface simplifiée (Java Webstart) qui ne nécessite pas d'installation.
- Une interface complète qu'il faut installer sur le poste récepteur.

- **Interface de configuration:** Elle permet de paramétrer de façon avancée le logiciel NAXFER. Notamment, de spécifier le proxy si la détection automatique a échoué, gérer les certificats d'authentification, définir des whitelists/blacklists pour la réception etc...

La réception se présente sous la forme d'un service (Windows) ou de démons (Linux ou MAC) qui gèrent les réceptions en parallèle et en tâche de fond ce qui permet à l'utilisateur de travailler sans se préoccuper des transferts.

Authentification

NAXFER établit un tunnel SSL entre un émetteur et un récepteur. Ce tunnel garantit l'identité de l'émetteur et du récepteur. Cette garantie passe par une authentification forte des deux parties.

Authentification des émetteurs: L'authentification de l'émetteur se fait depuis une clé USB (carte à puce) ou un fichier PKCS12 contenant le certificat X509 (RSA) de l'émetteur. Il s'agit d'une authentification forte à double facteur.

Authentification des récepteurs: L'authentification du récepteur se fait par défaut avec un certificat X509 public intégré dans l'interface de réception. Pour plus de sécurité, NAXFER permet également aux récepteurs de substituer leur propre certificat X509 qu'ils peuvent importer dans NAXFER depuis un fichier PKCS12.

Recherche du récepteur: Naxfer n'utilise pas les adresses IP pour localiser ses récepteurs. L'utilisateur dispose d'un annuaire internet, public ou privé, qui est mis à jour automatiquement par l'interface réception de NAXFER. Un mot de passe dédié à chaque société permet d'assurer la sécurité de l'annuaire. J&S CONCEPT peut également certifier l'identité d'un récepteur dans l'annuaire après enquête. En revanche, l'annuaire reste un moyen simple et intuitif de rechercher les destinataires d'un envoi mais ne constitue en aucun cas un moyen d'authentification.

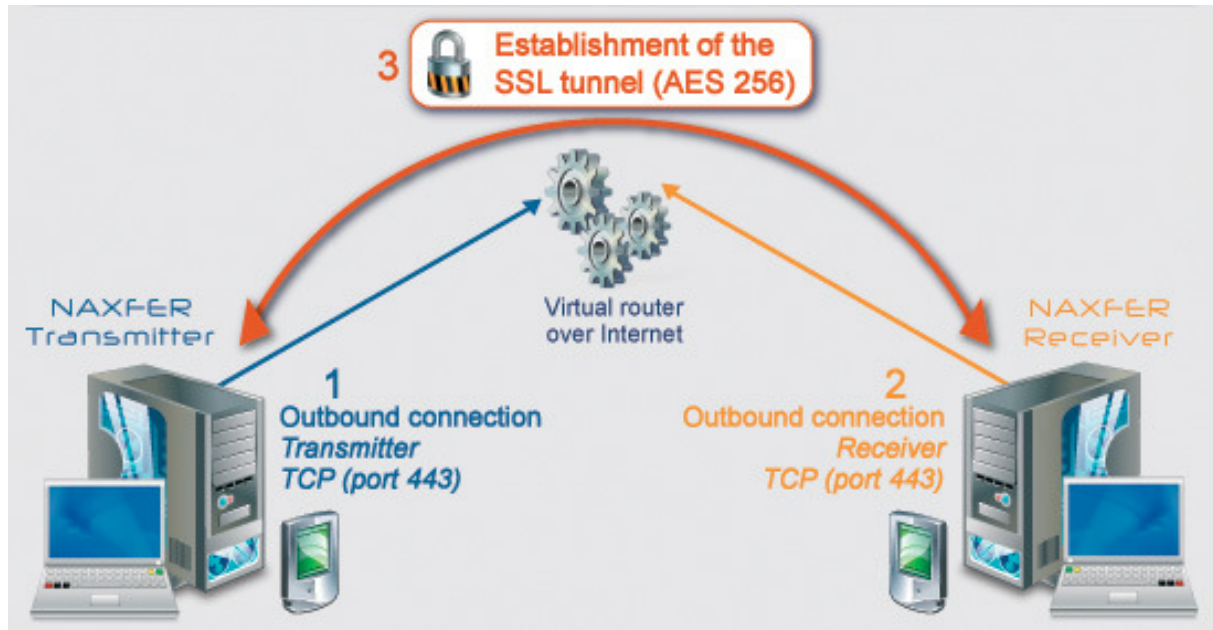
Protocole réseau et confidentialité

La communication via le réseau internet est au coeur de la technologie NAXFER. NAXFER s'adapte automatiquement aux réseaux privés ou publics en adoptant 2 modes de communication.

Les 2 modes sont les suivants :

- **Mode direct:** Ce mode s'applique lorsque l'émetteur et le récepteur se trouvent dans le même réseau local ou encore lorsque l'émetteur spécifie manuellement l'adresse IP du récepteur. Il consiste à établir une connexion TCP de l'émetteur vers le récepteur directement et à monter le tunnel VPN/SSL au dessus de cette connexion. Cette approche est déconseillée dans le cas où les deux parties ne sont pas dans le même réseau local car elle nécessiterait une intervention sur les parefeux et les routeurs du récepteur.

- **Mode “routeur virtuel”**: Le second mode utilise un “routeur virtuel” sur internet ou en DMZ pour établir la connexion selon le schéma ci-dessous :



Des connexions sortantes TCP sont établies sur le port 443, éventuellement à travers le proxy de l'entreprise, vers le routeur virtuel. L'émetteur et le récepteur établissent tous les deux le même type de connexion sortante. Ensuite, un tunnel VPN/SSL est négocié entre les deux parties à travers leur connexion TCP. Ainsi, tout le trafic qui transite par le routeur virtuel reste confidentiel. Le bénéfice premier de cette connexion TCP sur le port 443 est qu'elle est autorisée dans la majorité des entreprises et qu'elle ne présente pas une menace à la sécurité du réseau. Elle est équivalente à une connexion HTTPS via un navigateur.

Stockage des données sur le poste réception

Les données reçues par l'interface de réception sont cryptées en temps réel en mémoire avant leur stockage sur le disque dur.

Une clé de cryptage AES différente est utilisée pour chaque transfert. Cette clé est secrètement préservée sur le disque car elle est chiffrée avec le certificat X509 du récepteur. Par conséquent, en cas de vol de l'ordinateur du récepteur, les données qui n'ont pas été extraites sur le disque par l'utilisateur sont indéchiffrables sans le certificat de ce dernier qu'il peut avoir conservé dans une clé USB (carte à puce) par exemple.



Spécifications techniques

Authentification forte	Certificat RSA X509 (Client et Serveur) Clé matérielle + Pin
Méthodes de communication	SSL/TLS v1 on TCP/IP
Confidentialité	Chiffrement AES 256-bit
Non repudiation	Signature numérique et empreinte SHA1
Stockage des certificats	Zone privée, Clé USB HASP HL Time, Aladdin Ou toute carte à puce compatible PKCS11
Fournisseurs de certificats	J&S CONCEPT ou toute autorité de certification
Horodatage des transferts	Batterie autonome sur l'horloge de la clé HASP 4 à 6 ans d'autonomie
Mise à jour	Automatique par Internet
Langues disponibles	Français, Anglais, Espagnol
Langages de programmation	Java 1.5, C++



J&S CONCEPT | www.jnsconcept.com

15 cours Monseigneur Romero

91 000 EVRY, FRANCE

Tel : +33 1 60 79 85 57

Fax : +331 70 24 81 66

Email: contact@jnsconcept.com

