



Explication

Qu'est-ce que OFTP2 et quels sont ses avantages ?

OFTP, Protocole de Transfert de fichiers mis en place par ODETTE, a longtemps été le protocole de référence dans le domaine des échanges de données standardisés électroniques entre les partenaires commerciaux.

Les principaux composants lors d'un échange de données électroniques standardisé sont :

- Les informations proviennent d'applications différentes et sont mises sous forme de messages EDI standardisés.
- Les réseaux tels que ISDN, X25, TCP/IP (intranet/Internet (extranet) / VPN / ENX) utilisés pour transférer les données.
- Le Protocole OFTP qui contrôle le transfert des données grâce aux logiciels OFTP utilisés par l'expéditeur et le destinataire.

OFTP est un standard de facto au sein de secteurs industriels tels que l'Automobile, l'Ingénierie et le Transport. On l'utilise également pour des échanges de données avec des partenaires du secteur Public. Le système de données des douanes en Suède, par exemple.

Le Protocole OFTP a été créé par Odette, organisme de standardisation pour l'industrie automobile en Europe. La première version OFTP a été publiée en 1986. On pouvait l'utiliser avec les réseaux disponibles de l'époque, principalement les liaisons X25.

Pour Odette, les liaisons RVA (Réseau à Valeur Ajoutée) pouvaient s'intégrer dans la chaîne de communication.

Depuis 1986, le protocole OFTP a été publié en plusieurs versions, évoluant avec les changements de réseaux, avec l'introduction du réseau ISDN, X28 et X31 et plus récemment, le réseau Internet et VPN ENX (TCP/IP). La dernière version du protocole OFTP est la version 2, dite **OFTP2**. Cette version est principalement destinée aux échanges de données sécurisés sur Internet, où la sécurité est garantie grâce à l'utilisation de certificats.

La mise en œuvre du protocole **OFTP2** a démarré en 2009, en raison de facteurs suivants :

- Les anciens réseaux (X25/ISDN) ont été supprimés progressivement ou remodelés dans de nombreux pays.
- Le passage de réseaux anciens comme ISDN et X25 à des échanges de données sécurisés sur Internet permettra de réduire les frais de transport des données et d'augmenter considérablement la bande passante.
- **OFTP2** est la première solution utilisable dans le monde entier.



OFTP2 sécurisé

Les exigences de sécurité informatique en relation avec les échanges de données entre des partenaires varient en fonction du champ d'application. Voici quelques exemples d'informations que les utilisateurs souhaiteraient normalement protéger :

- Les données sur les produits et les données CAO.
- Les informations d'ordre financier.
- Les informations relatives à la tarification.
- Les informations concernant l'approvisionnement.

Puisqu'il est prévu d'utiliser **OFTP2** sur Internet essentiellement, il est nécessaire d'y ajouter de nouvelles techniques de sécurité non exigées pour les réseaux ISDN/X25.

Les principales sociétés automobiles ont convenu d'un niveau de sécurité considéré comme suffisant et fiable pour les processus commerciaux dans l'industrie automobile et dans d'autres secteurs.

Le niveau de sécurité choisi est élevé et équivaut à celui utilisé pour les paiements sur Internet. Les solutions sont basées sur l'utilisation de certificats.

Une session **OFTP2** est généralement plus complexe qu'un paiement normal sur Internet. C'est ce qu'il ressort des solutions de sécurité dans **OFTP2**.

OFTP2 a été développé avec l'active participation de la majorité des acteurs clés de l'industrie automobile ainsi que les principales sociétés de services (éditeurs). Ci-dessous apparaît le nom des industriels ayant soutenu OFTP2 dès le début :

BMW
BOSCH
DAIMLER
JCI
PSA
KARMANN
SCANIA
VOLKSWAGEN
VOLVO

À la fin de cette brochure, on trouvera des liens vers les sites des sociétés de service offrant des produits **OFTP2**.

Comment fonctionne OFTP2 ?

Le protocole OFTP a pour objectif d'exécuter et de contrôler les échanges de données entre les partenaires commerciaux. Certaines des fonctions les plus utiles du protocole OFTP sont :

- Établir une liaison directe entre les partenaires, après négociation initiale.
- Générer un accusé de réception.
- Reprendre les transferts de fichiers en cas d'échec.
- Échanger des informations électroniques sans aucune intervention humaine.

De plus, **OFTP2** apporte d'autres améliorations et de nouvelles fonctions :

- La compression des données.
- Facilite une communication sécurisée sur Internet entre les parties (SSL/TLS, authentification, signature, cryptage, etc.).
- Le traitement de très gros fichiers (> 500 GB).
- Une plus grande description de fichier.
- La disponibilité de jeux de caractères supplémentaires (Chinois et Japonais etc..).

OFTP2 est compatible avec les versions OFTP antérieures pour les connexions X25/ISDN, VPN ENX.

Quels sont les principaux avantages d'OFTP2 ?

Mondialisation de l'industrie automobile

De nombreuses sociétés opèrent internationalement dans le domaine des achats, de la fabrication et des ventes. Jusqu'à présent, il était nécessaire de choisir des solutions pour des échanges de données avec des partenaires soumis à des conditions régionales spécifiques (États-Unis, Europe, Asie, etc..).

Avec la globalisation d'Internet, il sera désormais possible d'utiliser la même solution partout. C'est non seulement vrai géographiquement parlant, mais aussi lorsqu'il s'agit de communiquer avec différents types de partenaires, des petits fournisseurs locaux aux grandes entreprises multinationales.

Changements de l'infrastructure des technologies de l'information

L'exemple illustrant de tels changements est l'arrêt définitif et/ou le remodelage des réseaux ISDN/X25. C'est déjà le cas dans les pays nordiques, en Allemagne et en France.

On constate, en même temps, que l'accès Internet est maintenant disponible presque partout. De nos jours, n'importe quelle société a plus ou moins accès à Internet comme étant l'un des services de leur Infrastructure informatique. Introduire **OFTP2** signifierait utiliser uniquement l'infrastructure disponible pour une autre fonction.



Même si la taille de l'infrastructure doit tenir compte de toute nouvelle application, l'introduction d'**OFTP2** ne devrait entraîner que de faibles coûts supplémentaires.

Changements des besoins en communication

La quantité de données transmises entre les partenaires n'a cessé de croître. Cela signifie qu'il est de plus en plus difficile d'utiliser les anciens réseaux à cause des bas débits et des modèles de tarification liée au volume.

On pourrait multiplier la vitesse de transmission par 25 si on passait de l'ISDN au réseau Internet 8 Mbits avec **OFTP2**. Ceci permettrait, par la même occasion, de réduire considérablement les coûts de service du réseau.

En utilisant la compression OFTP2, on réduirait encore plus le temps de transmission.

Avantages par rapport aux autres alternatives de communication (plus récentes)

OFTP2 est l'un des nombreux protocoles que l'on pourrait utiliser pour la communication EDI sur Internet. Les principaux protocoles "concurrents" sont les protocoles SFTP (Protocole de Transfert de Fichiers SSH) et AS2.

Avantages d'OFTP2 par rapport à ces protocoles :

- OFTP2 est le seul protocole capable de gérer des anciens réseaux comme X25/ISDN, mais aussi ENX et TCP/IP sur Internet.
- OFTP2 a été conçu pour faciliter la gestion de fichiers très volumineux (> 500 GB).
- Seul OFTP2 (et les versions précédentes de OFTP) ont des fonctions pour la reprise et l'accusé de réception.
- Seul OFTP2 (et les versions précédentes de OFTP) ont des fonctions de négociation et d'acceptation de la taille de fichier et de type de fichier.
- OFTP2 (et les versions précédentes de OFTP) est le seul protocole conçu pour gérer des échanges de données produit en utilisant la récente version 3 du message global ENGDAT EDI.

Que font les principaux acteurs ?

Bon nombre d'entreprises leaders en Europe sont déjà intéressées pour tester OFTP2 :

- DAIMLER, VOLKSWAGEN et BMW ont commencé à tester le protocole.
- SCANIA et VOLVO ont prévu de commencer les tests.
- PSA PEUGEOT CITROËN prépare le déploiement

ŠKODA AUTO est la première société à l'utiliser pour des échanges CAD réguliers depuis le 1^{er} avril 2009.



Quels sont les liens entre OFTP2 et les services réseaux ?

Tous les produits de communication qui supportent OFTP2, pourront gérer des échanges de données qui utilisent des versions précédentes d'OFTP et d'anciens réseaux comme ISDN, X31 et X25.

Par conséquent, rien ne devrait stopper les utilisateurs se préparant à recevoir de nouvelles exigences des partenaires qui mettent à jour leurs produits de communication vers une version prête pour OFTP2.

On peut s'attendre à ce que la migration s'étale dans le temps puisque tous les utilisateurs ne pourront ou ne souhaiteront pas migrer en même temps. Il y aura donc une période de transition pendant laquelle les deux versions seront utilisées en parallèle.

"OSCAR", le nouveau service d'identification d'Odette

OSCAR (Système de codage et d'enregistrement créé par Odette) attribue des codes uniques au niveau mondial à toute entreprise ou entité technique de l'industrie. Les codes OSCAR sont destinés à plusieurs fins, l'une d'entre elles étant l'identification de stations OFTP individuelles.

Le codage similaire est déjà en cours d'utilisation, mais avec OSCAR, il sera plus facile de maintenir un système mondial des codes des stations OFTP. Ce ne sera plus un problème de trouver un code approprié (code ICD), sur les marchés émergents par exemple.

Mise en œuvre

Par expérience, nous savons que certaines étapes sont nécessaires pour réussir une mise en œuvre :

Recueillir les informations :

- Obtenir de la documentation par le biais de GALIA.
- Participer, si possible, aux formations proposées par GALIA ou par les fournisseurs de solutions.
- Discuter de la mise en œuvre du protocole OFTP2 avec votre fournisseur de solution, compétent dans les domaines de la sécurité et des certificats.

Planning de migration et/ou nouvelle mise en œuvre :

- En cas de mise à jour de votre logiciel, ayez une discussion en interne et avec vos partenaires.
- En cas de demande de mise à jour, préparez un calendrier avec vos partenaires, votre fournisseur de logiciel et votre fournisseur de solution.
- Recueillez les informations pour savoir quand les versions antérieures seront remplacées.



Certificat de sécurité de la Solution

Il est important de clarifier les exigences des partenaires pour la sécurité de la solution :

- Le Certificat et les Autorités de Certification - Comment réduire le nombre d'options ?
- La politique de sécurité des Partenaires (cryptage de session, cryptage de fichiers, signature, accusé de réception).

Choisir un certificat

La confiance et la sécurité dans les transactions OFTP2 s'obtiennent en utilisant des certificats et tous les utilisateurs devront au moins avoir un tel certificat.

Les certificats sont délivrés et vendus par des sociétés spécialisées dites, "Autorités de Certification". Pour avoir une idée des Certificats et leur fonctionnement, rendez-vous sur le site :

http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique

Les utilisateurs sont assez libres de choisir leurs propres Autorités de Certification à condition de respecter les exigences des partenaires.

Pour éviter toute situation où les clients et les autres principaux partenaires demandent des solutions de certificat spécifiques, les membres d'Odette ont décidé d'accepter un nombre d'Autorités de Certification qui répondent à une liste de critères spécifiques.

Odette propose une liste des Autorités de Certification agréées (Listes de Statut - Service de Confiance, TSL). Ces informations sont disponibles sur le site <https://forum.odette.org/service/tsl-service>.

Cette liste contient les certificats reconnus comme étant "dignes de confiance", conformément à la politique des applications **OFTP2**. De nouvelles Autorités de Certifications seront ajoutées à cette liste, une fois validées par Odette.

Les principes de base de la liste de Confiance Odette sont :

- Les utilisateurs n'ont normalement à sélectionner qu'une seule Autorité de Certification de la liste pour obtenir des certificats d'utilisateur.
- Chaque utilisateur OFTP2 doit accepter des certificats de l'une des Autorités de Certification sur la liste TSL.

Ceci réduira considérablement les efforts administratifs de gestion des échanges de certificats.

Au sein de la communauté Odette, la première étape sera de sélectionner une Autorité de Certification de cette liste. La solution la plus simple serait de choisir Odette comme Autorité de Certification, et ainsi, vous n'aurez aucun problème pour trouver le bon service de sécurité. Vous pouvez également consulter la Liste de Confiance Odette pour voir quelles autres Autorités de Certification sont répertoriées comme celles de partenaires de l'industrie (DAIMLER, FORD, PSA, VOLVO, BOSCH etc..) ou de fournisseurs de services (VERISIGN, THAWTE).

Les utilisateurs doivent être conscients que les certificats pour OFTP2 peuvent gérer à la fois le "Serveur et l'Authentification du Client".

Si vous participez à la structure de sécurité Odette, vous n'aurez pas à discuter du niveau de sécurité pour les données échangées individuellement avec vos partenaires. Vous pourrez vous fier aux normes de sécurité définies au sein de l'industrie automobile.

Les partenaires s'accorderont sur les fonctions de sécurité (cryptage et signature de fichiers) qu'ils appliqueront pour leurs processus commerciaux au-delà d'une communication sécurisée.

Questions pratiques relatives à la mise en œuvre

Il y a des aspects qui, individuellement, ne doivent pas être si compliqués à gérer, mais qui pourraient encore soulever certaines questions. Il vous est donc recommandé de discuter des points suivants avec votre support technique et votre fournisseur de service :

Pare-feu

Le pare-feu devra être adapté pour OFTP2, port 3305 (OFTP) plus 6619 (TLS). Les ports doivent être ouverts dans les deux sens pour activer les numérotations entrantes et sortantes.

Adresse DNS (fixe) ou adresse IP

Nous vous recommandons de choisir une adresse IP fixe avec un nom DNS (oftp.supplier.com, par exemple) au lieu d'une adresse IP.

Cela devrait minimiser le risque de problèmes lors de changement d'opérateur (ISP).

Nous vous déconseillons l'utilisation de services DNS dynamiques sachant que cela vous obligerait à dépendre d'une tierce partie.



Certains services gratuits peuvent être fermés après 30 jours d'inactivité, par exemple si une adresse IP n'a pas été changée.

Adresse publique IP et connexion pour obtenir les certificats

Le nom DNS doit apparaître dans le certificat.

Tests

Choisissez bien votre partenaire pour les tests, la manipulation des certificats et autres.

Produits OFTP2

Il existe de nombreux logiciels OFTP2 disponibles. Cela va des logiciels très simples à 300 € environ avec une licence annuelle à moins de 100 €, à des produits plus complexes et plus onéreux contenant plusieurs modules de logiciels.

Afin de valider la conformité de ses produits spécifiques, Odette a introduit des tests d'interopérabilité **OFTP2**. Cliquez [ici](#) pour vérifier la liste des logiciels qui ont été testés. Pour plus d'informations, consulter notre site web www.odette.org ou le site web de GALIA www.galia.com.

Remerciements

Ce document a été réalisé par une équipe projet au sein d'Odette où sont représentées les sociétés et les organisations nationales suivantes :

DATAINTERCHANGE
FORD-WERKE GMBH
GALIA
HELLA
NUMLOG
ODETTE Espagne
ODETTE Suède
PIPECHAIN
SAP
SCANIA INFOMATE
TELEDIN
T-SYSTEMS ENTERPRISE SERVICES
VDA
VOLVO CARS IT
VOLVO IT