Comment choisir votre fournisseur de Cloud en toute confiance

CERTIFICATS THAWTE SSL : LE LIEN DE SÉCURITÉ ET DE CONFIANCE ENTRE VOUS ET VOTRE FOURNISSEUR DE CLOUD

Comment choisir votre fournisseur de Cloud en toute confiance

Introduction

Le paysage informatique traverse actuellement une profonde mutation marquée par l'avènement du Cloud Computing. De simple hypothèse, l'adoption du Cloud n'est désormais plus qu'une question de temps pour de nombreuses DSI. Les offres de Cloud externalisées (ou *cloud public*) suscitent l'intérêt marqué de nombreuses entreprises qui y voient un moyen de réduire leurs coûts et d'accroître leur flexibilité. Seul bémol, malgré ses formidables avantages économiques, le Cloud pose d'importants risques pour les entreprises soucieuses de protéger leur patrimoine informationnel d'une part, et de se conformer à un cadre réglementaire particulièrement dense d'autre part.

Pour répondre à ces impératifs de sécurité, les fournisseurs de services Cloud ont à leur disposition un certain nombre d'outils, au premier rang desquels on trouve les certificats SSL (*Secure Sockets Layer*). Leur mission : sécuriser les données qui transitent sur le Net. Ce document technique a pour but de proposer aux entreprises les éléments d'une réflexion pragmatique pour étayer leurs décisions. Pour les aider à déterminer le périmètre d'action et le calendrier d'adoption de solutions Cloud, nous passerons en revue les questions que les entreprises devront poser aux différents hébergeurs Cloud avant d'arrêter leur choix. Enfin, nous exposerons les avantages des certificats SSL délivrés par une autorité de certification (AC) de confiance pour les entreprises soucieuses d'aborder le virage du Cloud en toute sérénité.

Cloud Computing : nouvelles opportunités, nouveaux défis de sécurité

Pour la majorité des entreprises, la baisse des coûts constitue l'avantage n°1 du Cloud Computing, tant au niveau des dépenses d'investissement (CapEx) que des coûts d'exploitation (OpEx). Le Cloud se distingue également par sa flexibilité : capacités à la demande grâce au provisionnement en libre-service, mais aussi facturation à l'utilisation (« *pay-per-use* »). De son côté, le fournisseur de services Cloud réalise des économies d'échelles exponentielles en proposant à ses nombreux clients des ressources informatiques standardisées. Dans la course à la compétitivité, de nombreux hébergeurs traditionnels se sont déjà taillé une part du marché des services Cloud aux entreprises. Ils partent en effet avec l'avantage de posséder les compétences de base requises (ressources humaines, processus et technologies) pour faire profiter les entreprises des atouts du Cloud Computing.

Néanmoins, malgré les avantages économiques indéniables des services Cloud, les questions de sécurité, de conformité et de confidentialité ont, jusqu'ici, freiné leur adoption en entreprise. D'après une enquête IDC réalisée auprès de dirigeants informatiques, la sécurité arrive en tête de leurs préoccupations vis-à-vis des services Cloud[1]. Pour sa part, Gartner Research a identifié sept facteurs de risque de sécurité[2] associés au Cloud Computing en entreprise. De fait, lors du processus de sélection d'un fournisseur de Cloud, le cabinet recommande d'inclure ces points clés au cahier des charges.

- **Droits d'accès –** les fournisseurs de services Cloud doivent pouvoir attester de l'instauration de procédures d'embauche, de supervision et de contrôle d'accès adaptés à la délégation des opérations d'administration.

- **Conformité réglementaire –** les entreprises restent responsables de leurs données, même stockées dans un Cloud public. Elles doivent par conséquent s'assurer que les fournisseurs choisis sont prêts et disposés à se soumettre à des audits de contrôle.

QUE VOUS SOYEZ PRÊT OU PAS, LE CLOUD COMPUTING DÉBARQUE EN FORCE !

« Pour certains observateurs, le Cloud Computing constitue la révolution technologique la plus importante depuis l'avènement d'Internet. Pour d'autres, il ne s'agit que d'une mode passagère. En revanche, une chose est sûre : la technologie Cloud fait une percée fulgurante dans la liste des priorités des DSI. »

– Source : Gartner EXP Worldwide Survey (http://www.gartner.com/it/ page.jsp?id=1283413)

« L'adoption des services Cloud s'accélère en entreprise, à tel point que certains cabinets comme Gartner Research estiment qu'au cours des cinq prochaines années, les dépenses cumulées des entreprises dans les services Cloud devraient atteindre 112 milliards de dollars US à l'échelle planétaire. »

– Source : Gartner Research (http://www. gartner.com/it/page.jsp?id=1389313)

---

1. Source : IDC eXchange (http://blogs.idc.com/ie/?p=730)

2. « Assessing the Security Risks of Cloud Computing » (http://www.gartner.com/DisplayDocument?id=685308) Gartner, 3 juin, 2008.

- **Provenance des données –** à l'heure des choix, les entreprises ne doivent pas hésiter à interroger les hébergeurs sur la localisation de leurs datacenters et sur leur adhésion à une charte de confidentialité rigoureuse.

- **Ségrégation des données –** la plupart des Clouds publics sont hébergés dans des environnements mutualisés. Dans ce contexte, les hébergeurs doivent pouvoir garantir une ségrégation totale des données, pour une sécurisation complète sur une architecture multi-locataires (« *multi-tenant* »).

- **Restauration des données –** en cas de sinistre, les entreprises doivent s'assurer que leur hébergeur sera capable de restaurer l'intégralité de leurs données.

- **Surveillance et reporting –** la surveillance et la journalisation de l'activité du Cloud public constituent des opérations délicates. Il incombe donc aux entreprises de vérifier que leur fournisseur d'hébergement est en mesure de procéder aux investigations nécessaires.

- **Continuité de service –** les hébergeurs vont et viennent. Leurs clients doivent par conséquent se renseigner de manière concrète sur la portabilité de leurs données, pour d'une part éviter tout phénomène d'enfermement, et d'autre part se prémunir contre la perte de données en cas de faillite du prestataire.

Pour exploiter toutes les potentialités du Cloud Computing sans compromettre leur sécurité et leur conformité, les entreprises feront donc exclusivement appel à des fournisseurs de confiance, capables d'agir sur les questions de sécurité dans le Cloud en général, et sur ces sept points en particulier. Autre facteur de complication, lorsqu'elles passent d'un opérateur unique à des services Cloud multi-fournisseurs, les entreprises doivent gérer ces questions avec plusieurs opérateurs dotés d'infrastructures, de politiques d'exploitation et de compétences différentes en matière de sécurité. Devant la complexité des enjeux de confiance autour du Cloud, les entreprises doivent pouvoir s'appuyer sur une méthode universelle et fiable pour sécuriser leurs données en transit vers le Cloud, en provenance du Cloud ou en périphérie du Cloud.

SSL : la clé d'un Cloud Computing sécurisé pour l'entreprise

Utilisé par les navigateurs et serveurs Web, SSL est un protocole de sécurité qui protège les données transférées sur Internet. À ce titre, SSL s'impose comme la norme de référence pour l'échange sécurisé d'informations sur la Toile. Sans l'universalité du SSL, la confiance sur Internet resterait lettre morte. À chaque déplacement de données, le protocole SSL entre en jeu. Si une entreprise conserve ses données dans le Cloud, il est essentiel qu'elle dispose d'un accès réseau sécurisé. Les données sont également susceptibles de transiter entre différents serveurs d'un même Cloud, notamment lors des opérations de maintenance menées par le fournisseur. Peu importe la nature des mouvements de données (serveur/navigateur ou serveur/serveur), le protocole SSL en assure la sécurité.

Deux services SSL apportent une réponse à certains points d'interrogation concernant la sécurité dans le Cloud. Tout d'abord, le cryptage SSL protège les données des regards indiscrets, tant lors des transmissions de serveur à serveur que de serveur à navigateur. Autre avantage, et non des moindres, le protocole SSL atteste de l'authenticité et du sérieux d'un serveur et d'un domaine donnés. De fait, un certificat SSL authentifie l'appartenance d'un serveur et d'un domaine spécifiques à la personne morale ou physique qui en revendique la propriété. Pour cela, le fournisseur d'hébergement doit utiliser un certificat SSL délivré par une autorité de certification (AC) indépendante.

Ségrégation des données et sécurisation de l'accès aux services Cloud

En matière de stockage dans le Cloud, les risques d'une éventuelle absence de ségrégation des données sont omniprésents. Dans un modèle traditionnel de stockage sur site, le responsable contrôle précisément l'emplacement des données et les personnes autorisées à y accéder. Dans un environnement Cloud, le scénario est radicalement différent car c'est le fournisseur du service Cloud qui contrôle l'emplacement des serveurs et des données. Une mise en œuvre appropriée des technologies SSL permet toutefois de sécuriser les données sensibles lors de leurs déplacements au sein du Cloud, entre les serveurs du fournisseur de Cloud et vers les navigateurs des utilisateurs.

CRYPTAGE

Les entreprises doivent exiger de leur fournisseur de Cloud qu'il associe le protocole SSL à des serveurs prenant en charge un cryptage 256 bits minimum, pour une sécurité renforcée. Ce faisant, les données en transit serveur/serveur ou serveur/navigateur bénéficient d'un niveau de cryptage conforme, voire supérieur aux standards en vigueur. L'entreprise prévient ainsi toute interception ou consultation des données par des personnes non autorisées.

AUTHENTIFICATION

Les entreprises doivent également exiger que le propriétaire de chaque serveur soit authentifié avant que le moindre bit de données ne soit transféré entre serveurs. Les certificats SSL autosignés n'ont aucune valeur en termes d'authentification. Seuls les certificats SSL délivrés par un organisme indépendant sont en mesure d'authentifier légitimement le propriétaire d'un serveur donné. Aussi, pour empêcher que l'environnement du fournisseur Cloud ne soit infiltré par un serveur « pirate », l'entreprise devra exiger la présence d'un certificat SSL délivré par une autorité de certification indépendante ayant préalablement authentifié le serveur.

VALIDITÉ DU CERTIFICAT

Une fois le serveur et le domaine authentifiés, le certificat SSL émis pour cet équipement reste valable pour une durée définie. Dans les rares cas de compromission d'un certificat SSL, l'on peut néanmoins vérifier que le certificat n'a pas été révoqué depuis son émission initiale. Chaque fois qu'une négociation SSL (*handshake*) est initiée, le certificat SSL fait l'objet d'une vérification via un contrôle de la base de données des certificats révoqués.

Ce contrôle de validité s'appuie sur deux standards : le protocole OCSP (*Online Certificate Status Protocol*) et la liste CRL (*Certificate Revocation List*). Avec le contrôle OCSP, une requête est envoyée à l'autorité de certification pour demander si le certificat concerné a été révoqué. L'AC répond par oui ou par non. Dans la négative, la négociation SSL peut alors commencer. Dans le cadre d'un contrôle CRL, le navigateur doit télécharger la dernière liste de révocation en date auprès de l'autorité de certification et vérifier, par lui-même, si le certificat figure sur cette liste.

La méthode de contrôle OCSP est généralement considérée comme étant la plus fiable. Réactualisé en permanence, ce contrôle est moins sujet aux déconnexions (*timeout*) provoquées par l'encombrement des réseaux. Les certificats SSL contrôlés exclusivement via la méthode CRL sont moins prisés car en cas de saturation du réseau, il arrive que l'étape de contrôle soit purement et simplement abandonnée. Certains navigateurs interprèteront alors l'absence de contrôle CRL comme la confirmation que le certificat ne figure pas sur la liste de révocation. Résultat : les négociations SSL sont entamées et la session démarre sur la base d'un certificat SSL révoqué. Dans ce type de scénario, un serveur frauduleux peut utiliser un certificat révoqué pour se faire passer pour légitime, et créer ainsi les conditions idéales pour une violation des données.

Levier de conformité réglementaire

Autre facteur de risque : le non-respect des obligations réglementaires. En matière de sécurité et de confidentialité des données, les entreprises croulent sous le poids des réglementations : aux États-Unis, les lois Sarbanes-Oxley (SOX) s'appliquent aux entreprises publiques, le standard PCI-DSS (*Payment Card Industry Security Standard*) régit toutes les sociétés qui acceptent les paiements par carte, et la loi HIPAA (*Health Insurance Portability and Accountability Act*) vise tout organisme ou entreprise susceptible d'être en contact, de près ou de loin, avec les données des patients. L'UE a pour sa part adopté la Directive européenne pour la protection des données à caractère personnel, dont la loi PIPEDA (*Personal Information Protection and Electronic Documents Act*) représente l'équivalent au Canada.

MODE DE FONCTIONNEMENT DU PROTOCOLE SSL

Un certificat SSL contient une paire de clés publique et privée, ainsi que des éléments d'identification vérifiés. Lorsqu'un navigateur (ou un client) entre en relation avec un domaine sécurisé, le serveur partage sa clé publique (par le biais du certificat SSL) avec le client pour établir une méthode de cryptage et une clé de cryptage unique pour la session en question. Le client confirme qu'il reconnaît et fait confiance à l'émetteur du certificat SSL. Adossé à une architecture backend ultra évoluée, maillée de contrôles et de doubles-vérifications de sécurité, ce processus baptisé négociation SSL (*SSL handshake*) marque l'ouverture d'une session sécurisée protégeant la confidentialité et l'intégrité des données.

Même si elle externalise une partie de son informatique dans le Cloud, l'entreprise est tenue de veiller à son respect des lois SOX et HIPAA, du standard PCI et des autres réglementations en vigueur – avec les ajustements que cela suppose, suivant la localisation des serveurs et des données. En d'autres termes, l'externalisation de l'informatique ne modifie en rien la responsabilité de l'entreprise vis-à-vis de la sécurité et de l'intégrité de ses données. Le responsable informatique de l'entreprise ne peut s'appuyer uniquement sur son fournisseur de Cloud pour satisfaire à ces exigences. De fait, il doit exiger de ce fournisseur qu'il se soumette à des contrôles de conformité externes. Pour les fournisseurs de Cloud Computing, refuser de se prêter au jeu des audits externes et des certifications de sécurité revient à dire à leurs clients « [qu'ils] ne peuvent solliciter leurs services que pour les fonctions les plus triviales », selon Gartner.

Autre point important, les modifications technologiques apportées à l'environnement Cloud Computing du fournisseur peuvent affaiblir, malgré elles, la conformité réglementaire et juridique du client. Autres éléments susceptibles d'affecter cette conformité : les mises à niveau fonctionnelles telles que les modifications d'autorisation, l'ajout de nouvelles fonctionnalités, l'introduction de terminaux mobiles et les changements au niveau du réseau[3]. À l'instar de la ségrégation des données, le cryptage SSL empêche toute divulgation des données protégées ou confidentielles, grâce à l'automatisation du processus de *due diligence* réglementaire et de l'accès aux données. Le cryptage SSL rend les informations illisibles et inutilisables par toute personne non autorisée qui chercherait à les intercepter ou les consulter.

Traçabilité des données

Troisième facteur de risque : la localisation des données. Là encore, le protocole SSL apporte une réponse à ce problème. Les Clouds publics présentent de nombreuses similitudes avec les « *black boxes* » : s'ils garantissent un accès universel aux données, ils peuvent parfois masquer l'emplacement physique des serveurs et données. Or, si le fournisseur de Cloud applique un cryptage SSL aux données en transit, le propriétaire des données peut être rassuré quant à la sécurité de ses données au fil de leurs pérégrinations dans le Cloud.

3. « Domain 10: Guidance for Application Security V2.1, » Cloud Security Alliance, juillet 2010.

De plus, un fournisseur SSL indépendant et réputé comme Thawte n'émettra aucun certificat SSL à un serveur basé dans un pays frappé d'interdictions, comme la Corée du Nord et l'Iran notamment. Par conséquent, dès lors que le fournisseur de Cloud exige l'authentification et le cryptage SSL sur l'ensemble de ses serveurs via une autorité de certification de confiance, les entreprises clientes de ce fournisseur auront l'assurance que leurs données ne seront pas stockées sur des équipements informatiques basés dans ces pays.

Autres atouts du SSL

L'entreprise doit savoir par quels moyens son fournisseur de Cloud – qui possède des serveurs partout dans le monde – protège ses données en cas de sinistre. Gartner indique à ce propos que « toute offre non assortie d'une réplication multi-sites des données et de l'infrastructure applicative présente un risque de panne totale ». Toujours selon le cabinet, toute entreprise dans le Cloud a le devoir de s'informer sur la capacité de son fournisseur à restaurer l'intégralité de ses données à partir de sauvegardes ou de réplications, et sur la durée d'une telle opération. Pour éviter tout risque de perte de données, les fournisseurs de services Cloud doivent également conserver des référentiels de sauvegardes des données. En cas de panne, les hôtes du Cloud tenteront de restaurer leurs données à partir des serveurs de sauvegarde. Avec les certificats SSL, le processus de sauvegarde et de restauration bénéficie d'une couche de protection supplémentaire : les données issues des serveurs de sauvegarde ou des serveurs dupliqués sont cryptées pendant leur transfert. De plus, les serveurs hébergeant ces sauvegardes de données sont authentifiés comme étant des sources d'information légitimes.

Certificats SSL : gage de confiance dans le Cloud

L'entreprise qui fait appel à un fournisseur de services Cloud doit pouvoir lui accorder toute sa confiance. Ses applications métiers critiques ne souffrent, en effet, aucun empirisme ni improvisation. Les DSI doivent par ailleurs insister sur l'importance du critère de fiabilité comme levier de confiance. Les certificats SSL constituent, à ce titre, un moyen visible et immédiatement reconnaissable de parvenir à cette fin. Inversement, l'absence de certificat SSL, ou la compromission d'un certificat SSL, peuvent instantanément réduire cette confiance à néant.

Exemple : imaginons qu'une entreprise héberge son site marchand dans le Cloud public et que son fournisseur rencontre un problème avec le certificat SSL du site. Les visiteurs sont aussitôt accueillis par un message d'erreur du type « Échec de la connexion sécurisée » ou « Le certificat de sécurité du site Web pose problème.». Les internautes passeront-ils outre ces avertissements pour effectuer une transaction sur un site visiblement peu fiable ? Ce n'est guère probable.

La chaîne de confiance englobe le fournisseur de Cloud et s'étend jusqu'à son partenaire de sécurité. La sécurité proposée par le fournisseur de Cloud correspond, ni plus, ni moins, au niveau de fiabilité de la technologie de sécurisation utilisée. Les hébergeurs doivent par conséquent opter pour les certificats SSL d'une autorité de certification connue, fiable, sûre et indépendante. Par ailleurs, le niveau de cryptage recommandé est de 256 bits. Quant au processus d'authentification, il doit être extrêmement rigoureux.

Certains fournisseurs génèrent leurs clés SSL via des serveurs sous Debian. Or, les fonctionnalités de base de cryptage de ce système ont fait l'objet d'attaques entre 2006 et 2008. Les entreprises doivent donc s'assurer que leur fournisseur de Cloud n'utilise aucun serveur ou certificat SSL susceptible d'avoir été compromis par cette faille de sécurité. La durée de validité maximale des certificats SSL étant de six ans, le risque de tomber sur un certificat SSL infecté reste possible[4].

AUTHENTIFICATION : UN GAGE DE CRÉDIBILITÉ POUR LES HABILITATIONS

La crédibilité d'une habilitation dépend de la confiance dont bénéficie l'organisme émetteur, car c'est ce dernier qui atteste de l'authenticité de l'habilitation. En ce sens, les autorités de certification disposent de plusieurs méthodes de vérification des informations transmises par les entreprises.

La solution idéale consiste à choisir un fournisseur de Cloud ayant consolidé ses certificats SSL autour d'une seule et même autorité de certification, réputée pour son sérieux auprès des éditeurs de navigateurs. Ce fournisseur devra également appliquer une méthodologie d'authentification rigoureuse et gérer une infrastructure fiable. Il existe quatre niveaux d'authentification pour le SSL. Le cryptage des échanges d'informations est prévu dans tous les cas. La différence réside dans la « puissance » de l'authentification du serveur et du domaine. En d'autres termes, les niveaux d'authentification dépendent des efforts déployés pour valider la propriété et le degré de contrôle d'un serveur ou domaine.

- Les **certificats autosignés** permettent uniquement de crypter les informations, rien de plus. Ce type de certificat SSL n'offre pas le niveau de sécurité requis par les entreprises.

- Les **certificats de validation de domaine** n'offrent qu'un niveau d'authentification de base. Cette solution d'entrée de gamme confirme uniquement le droit du demandeur à utiliser un nom de domaine donné. Ces certificats ne sont pas recommandés pour les connexions serveur/navigateur car ils ne contrôlent ni n'affichent l'identité de l'entreprise responsable de ce domaine ou serveur.

4. Source : http://voices.washingtonpost.com/securityfix/2008/05/debian_and_ubuntu_users_fix_yo.html

- Les **certificats de validation de l'organisation** offrent un niveau d'authentification fiable pour le Cloud. Ils confirment en effet l'existence de l'entité qui revendique la responsabilité du domaine ou du serveur en question, et l'habilitation de la personne sollicitant le certificat SSL pour le domaine ou serveur à agir au nom de cette entité. Ces certificats SSL constituent une solution acceptable pour les connexions serveur/navigateur. Toutefois, ils n'offrent pas le niveau de confiance maximum pour l'utilisateur.

- Les **certificats Extended Validation (EV)** représentent l'option de choix pour les connexions serveur/navigateur. Ils offrent en effet le niveau d'authentification maximum, accompagné d'une garantie immédiate et visible de la sécurité de la connexion. Ces certificats à validation étendue (EV) vérifient l'existence juridique, physique et opérationnelle de l'entité contrôlée, ainsi que le droit de cette entité à utiliser le domaine concerné. La procédure EV garantit que l'identité de l'entité a été vérifiée dans les enregistrements officiels d'un organisme agréé et indépendant, et que la personne requérant le certificat est dûment habilitée à le faire par l'entité concernée.

Un certificat SSL assorti de ce niveau d'authentification maximum déclenche l'affichage de marques d'identification extrêmement claires dans le navigateur de l'internaute : la barre d'adresse s'affiche en vert et indique le nom de l'entité détentrice du certificat SSL, ainsi que le nom de l'AC émettrice. Lorsqu'un internaute aperçoit la barre d'adresse verte, il sait immédiatement que sa connexion est sécurisée. Une fois leurs certificats SSL EV déployés, de nombreuses entreprises ont constaté une augmentation sensible du nombre de transactions effectuées sur leur site. Pour toutes ces raisons et bien d'autres, EV constitue la solution à privilégier pour l'hébergement d'applications et de services dans le Cloud.

Conclusion : ne partez pas dans l'inconnu

Pilier de la sécurité dans le Cloud, la technologie SSL a plus que fait ses preuves. Au moment de choisir un fournisseur de Cloud Computing, l'entreprise devra passer à la loupe les niveaux de sécurité mis en place par ce dernier. L'utilisation de certificats SSL émis par une autorité de certification réputée contribue fortement à garantir l'image de sérieux du fournisseur, ainsi que son engagement à protéger les données qui lui sont confiées. Les entreprises devront également se montrer très fermes sur les obligations du fournisseur en matière de gestion et de réduction des risques sortant du champ d'action du SSL. Lors de l'évaluation des différentes solutions de Cloud Computing, et avant de s'engager contractuellement, les entreprises passeront donc en revue les sept points clés recensés par Gartner.

Les certificats SSL déployés par les fournisseurs de Cloud devront par conséquent être délivrés par une autorité de certification connue, fiable, sûre et indépendante. Par ailleurs, ces certificats devront fournir un cryptage 256 bits basé sur la nouvelle racine globale de 2 048 bits. Le processus d'authentification devra, quant à lui, être extrêmement rigoureux. Pour garantir une protection et une disponibilité maximales des données, l'autorité émettrice de certificats SSL assurera une sécurité de type « défense nationale » dans ses datacenters et sites de secours. Chaque année, l'autorité de certification SSL devra faire auditer ses pratiques d'authentification par un organisme indépendant de confiance. Les produits SSL proposés par Thawte répondent à toutes ces exigences.

Pour en savoir plus, contactez nos conseillers commerciaux :

- **Par téléphone**
  - **États-Unis : +1 888 484 2983**
  - **Royaume-Uni : +44 203 450 5486**
  - **Afrique du Sud : +27 21 819 2802**
  - **Allemagne : +49 69 3807 89081**
  - **France : +33 1 57 32 42 68**
- **Par e-mail : Enterprisesales@thawte.com**
- **Sur notre site Web : http://www.thawte.fr/ssl/volume-discount-ssl-certificates/index.html**

Protégez votre activité et inspirez confiance à vos clients grâce à la sécurité renforcée des certificats numériques signés Thawte, leader mondial de la sécurité en ligne. Stabilité, fiabilité, infrastructure éprouvée, support client irréprochable… en 17 ans, Thawte a su s'imposer comme le partenaire international de choix pour les entreprises du monde entier.

UID 190/2/13