Opérateur national de services de confiance

KEYNECTIS

www.keynectis.com

Siège social : 30, rue du Château des Rentiers • 75647 Paris Cedex 13 • France • Tél. + 33 (0)1 53 94 22 00 • Fax : + 33 (0)1 53 94 22 01 • **www.keynectis.com**

S.A. au capital de 6 860 956 Euros • RCS Paris B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

SOMMAIRE

1 PRESENTATION DE LA SOCIETE

Nom : KEYNECTIS

Date de création : Juillet 2004

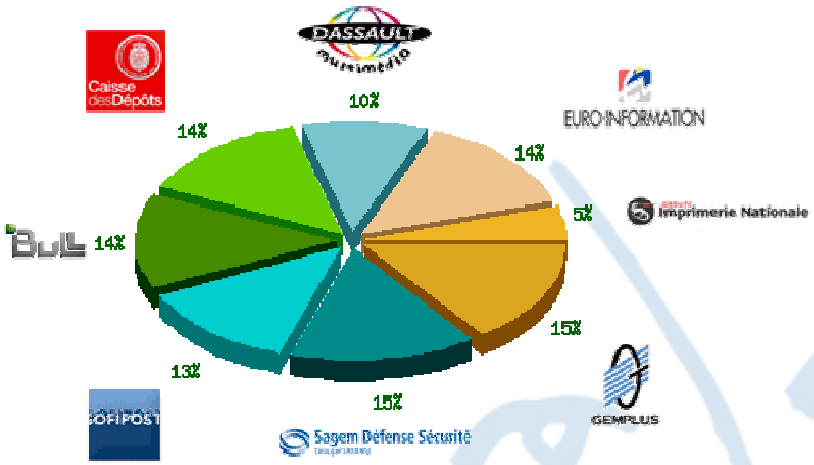
Activité : Opérateur de services de certification électronique, Infrastructures de Gestion de Clés (IGC), Infrastructure à Clés Publiques (ICP), Public Key Infrastructure (PKI), signature électronique, horodatage électronique

Effectif : 35 personnes

Siège social
30, rue du Château des Rentiers
75647 Paris Cedex 13 - France
Tel.: +33 (0)1 53 94 22 00
Fax: +33 (0)1 53 94 22 01
www.keynectis.com

Nature et répartition du capital social

La société KEYNECTIS est une société anonyme au capital social d'environ 7 millions d'euros répartis entre les actionnaires suivants:



Monsieur Thierry DASSAULT assure la présidence du Conseil d'Administration.

Eléments fondateurs de KEYNECTIS

La société KEYNECTIS est née du rapprochement des 2 opérateurs français des services de confiance, Certplus et PK7. La naissance de l'opérateur relève de 2 facteurs majeurs :

- Disposer d'une infrastructure technologique européenne capable de répondre aux besoins des grands projets
- Constituer un pôle d'expertise reconnu au plan européen, capable de faire face à la concentration des acteurs du marché

Reflet de ses multiples compétences, les prestations s'organisent en deux types de services :

- Externalisation de services d'Infrastructures de Clés Publiques (ICP ou PKI)
- Mise en place, supervision et maintenance de plates-formes PKI sur le site du client

2 LA VALEUR AJOUTEE DE L'OPERATEUR KEYNECTIS

La dématérialisation, c'est-à-dire la transposition sous format électronique des échanges traditionnels réalisés au quotidien (contrats, courriers, factures, formulaires administratifs…) est avant tout un moyen de fluidifier les processus métier.

Amorcés notamment au travers de projets de l'administration autour de la volonté de dématérialisation des procédures, les projets de dématérialisation couvrent principalement le transfert de résultats comptables, la déclaration de données sociales et la déclaration et la paiement en ligne de la TVA pour les grandes entreprises ou la déclaration de revenus pour les contribuables français.

Concernant pour l'heure plusieurs centaines de milliers d'utilisateurs, l'utilisation des procédures dématérialisées s'étend à l'ensemble des entreprises françaises, le cadre juridique ayant consacré la valeur juridique d'un document sous forme électronique.

Ainsi, de très nombreuses entreprises ont dématérialisé certains de leurs échanges, comme par exemple :
- Signature électronique de flux comptables entre entités d'un même groupe,
- Connexion d'un commercial itinérant au système d'informations de son entreprise pour passer des commandes en ligne ou télécharger des informations,
- Connexion sécurisée à un Extranet par les clients, fournisseurs ou partenaires d'une société.

Les aspects novateurs et techniques de ces applications imposent la nécessité, pour l'entreprise, de faire appel à des prestataires de services spécialisés et capables de jouer le rôle de tiers de confiance - en vue, le cas échéant, de fournir la preuve de l'échange.

Au centre des technologies utilisées : le certificat électronique
Véritable passeport électronique, indissociable des notions de signature électronique et de chiffrement, le certificat électronique permet d'authentifier les parties prenantes d'un échange électronique.

Pour disposer de leur service de confiance, les Tiers de Confiance (Autorité de Certification, Autorité d'Horodatage, Autorité de Validation) aussi bien que les entreprises ou organisations s'appuient sur l'unité de production de KEYNECTIS, qui assure la gestion technique du service.

Pionnier en la matière, KEYNECTIS est un Opérateur de Services de Confiance; industriel, il se met au service d'une ou de plusieurs entités désireuses d'offrir des services de confiance et laisse à celles-ci (devenues Autorités) un contrôle total sur les modes d'attribution, de diffusion et de gestion des certificats numériques.

La production des certificats, processus consistant en un ensemble d'opérations techniques: manipulations d'équipements informatiques et cryptographiques, personnalisation de cartes à puce, utilisation d'annuaires et de bases de données, se trouve ainsi confiée à un acteur de confiance dont c'est le métier. Toutes ces tâches requièrent en particulier des expertises technologique, juridique et sécuritaire afin d'assurer à l'Autorité de Certification que les certificats émis sont bien ceux souhaités, et qu'ils sont produits dans les délais et conditions de sécurité requis.

2.1 Notre savoir-faire

Le recours à KEYNECTIS, acteur spécialisé, pour la mise en œuvre d'un service de certification électronique doit être vu comme la 'location' d'un outil de délivrance de ce service et des prestations associées.

Au travers d'un co-pilotage approprié et d'un véritable partenariat conclu entre l'entreprise cliente (ou partenaire) et KEYNECTIS, vous bénéficiez de la qualité constante du service de KEYNECTIS, de son expérience et de sa notoriété.

Dans la pratique, KEYNECTIS vous apporte les avantages suivants :

- Mise en place d'un service innovant et industrialisé en moins de 3 mois,
- Mise à disposition et utilisation d'un outil éprouvé,
- Maîtrise du service et de l'infrastructure associée,
- Garantie de la qualité de service de KEYNECTIS,
- Maîtrise des investissements et coûts associés, au travers notamment du principe de mutualisation des services,
- Usage d'un outil évolutif, soit pour s'adapter aux besoins de changement de l'entreprise, soit pour tenir compte des évolutions techniques, technologiques, normatives ou réglementaires.

2.2 Le centre de production de KEYNECTIS

Le site de production de KEYNECTIS, comme tout site industriel, fait l'objet d'une attention de tous les instants. **Dédié au métier d'opérateur de confiance** et il se doit d'être à même de tenir compte des évolutions, tant en terme technique, qu'en terme de législation applicables (droit du travail, encadrement des nouvelles technologies…).

2.2.1 Une analyse de risque qui permet de maîtriser l'innovation

Opérer un site industriel au profit de clients pour y héberger leurs applications de confiance nécessite non seulement de faire le choix d'utiliser des matériels et technologies performants, mais aussi de prendre la mesure de l'ensemble des évènements susceptibles de contraindre son fonctionnement voire de le dégrader et remettre en cause les engagements de services conclus.

Dans ce sens, KEYNECTIS a, depuis sa création, réalisé et tenu à jour les analyses de risques du métier d'opérateur de certification qui s'imposent. Son choix s'est porté sur l'utilisation de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) initialement développée par la DCSSI pour couvrir les besoins gouvernementaux du domaine

2.2.2 Une complète orientation vers la délivrance de services de confiance électronique

Le centre et les moyens mis en œuvre par KEYNECTIS ont pour vocation initiale la génération de certificats électroniques.

Dans la pratique, ils vont bien au-delà et permettent à eux seuls de supporter la mise en place complète de vos espaces de confiance et la génération des éléments de preuve qu'ils requièrent.

Ces services incluent :

- La gestion du cycle de vie des autorités de certification,
- La gestion du cycle de vie des certificats numériques,
- La publication des éléments associés de la gestion de ces cycles de vie,
- La production de jetons d'horodatage,
- La personnalisation des cartes à puces et autres clés USB,
- La vérification de signature électronique ou de la validité de certificats…

2.2.3 Une sécurité de haut niveau à votre service

Le niveau de sécurité du centre industriel de KEYNECTIS est directement issu des analyses de risques réalisées par KEYNECTIS. Il est régulièrement évalué au travers d'audits tiers effectués par des professionnels du domaine. Leurs éventuelles observations sont immédiatement utilisées pour mettre à jour et/ou définir les plans d'action sécurité annuels du centre, afin d'apporter toujours plus de confiance dans la fourniture de nos prestations.

2.2.4 Une totale maîtrise de l'outil et des procédures organisationnelles

Les engagements de KEYNECTIS vis à vis de ses clients visent à garantir non seulement la délivrance des services de certification électronique dans des conditions de sécurité appropriées (disponibilité, intégrité, confidentialité, preuve), mais aussi les performances de délivrance de ces services (débit, temps de réponse…), leur constance et la capacité de prévenir, détecter, corriger toute anomalie selon des routines éprouvées et dans la plus grande transparence vis à vis des clients.

A cet effet, KEYNECTIS a mis en place et tient à jour un système de gestion de la qualité qui précise l'ensemble des processus liés à la délivrance de ces services et leurs enchaînements. Ce système de gestion de la qualité est disponible au personnel de KEYNECTIS disposant du besoin d'en connaître et évolue selon les besoins, nécessités et recommandations éventuelles des auditeurs tiers.

2.2.5 Une maîtrise des processus métiers (gestion de configuration, maîtrise de la maintenance)

Pour assurer la constance de ces services, KEYNECTIS inscrit la prise en compte des évolutions de son outil et de ses pratiques dans un schéma classique de gestion de la configuration et des changements auxquels ses clients sont mêlés. Toute mise en place de changement ou mise à jour, fait l'objet de vérifications (bon fonctionnement, non régression…) et de planification, la capacité de retour étant elle-même conservée.

2.2.6 Une forte orientation vers le client (service client, support technique, gestion des incidents)

Point de départ de la délivrance des services de KEYNECTIS, le client reste un élément central pendant toutes les étapes de son partenariat avec KEYNECTIS, que ce soit lors de la phase de spécification du projet, lors de mise en place ou pendant sa phase d'exploitation (délivrance des services par KEYNECTIS). A cet effet, un point contact unique lui est attribué auprès duquel toutes ses requêtes sont prises en compte pour traitement.

2.2.7 Maîtrise stratégique de l'infrastructure par le client

Les besoins en service de certification de chacun sont d'une telle sensibilité qu'il peut paraître insolite de vouloir les confier à un acteur tiers, même si celui-ci est un spécialiste du domaine. C'est pourquoi KEYNECTIS opère une technologie et a développé des procédures qui conservent à ses clients une maîtrise et une visibilité complètes des tâches sensibles de la mise en place et de l'opération des services pour lesquels il a opté.

Cette maîtrise, à base de partage de moyens, de rôles, de responsabilités, de traces et de transparence, assure entre autres que KEYNECTIS ne réalise aucune opération sans le consentement et/ou la participation/supervision du client.

2.3 La technologie d'opérateur

L'émission et la gestion du cycle de vie des certificats électroniques, surtout en masse, constituent un métier d'expertise à très forte valeur ajoutée, nécessitant notamment une infrastructure de haute sécurité et un savoir faire d'exploitation très spécifique, lié à de fortes contraintes sécuritaires.

Le logiciel SEQUOIA® se caractérise par :
- Sa capacité à gérer en parallèle un grand nombre de contextes (AC, AE, gabarits de certificats, …) en mutualisant les ressources techniques et humaines
- Sa forme générique permettant de répondre à un nouveau besoin, par simple paramétrage, en peu de temps et peu d'effort
- Son haut niveau de performance et de robustesse
- Son architecture basée sur les techniques les plus récentes
- Son respect des standards les plus répandus (X509 v3, PKCS, XML, SOAP, SAML, LDAP).

Le logiciel SEQUOIA® est constitué d'un noyau, disposant des fonctionnalités essentielles d'une ICP, auquel peuvent s'ajouter des fonctionnalités additionnelles pouvant adresser aussi bien des besoins simples et génériques que des besoins complexes et spécifiques :

- Un cœur d'Autorité de Certification mutualisé supportant différents types de ressources cryptographiques (HSM BULL TrustWay, Safenet LUNA CA, CA3 et SA) et permettant de gérer de multiples AC au sein de domaines de confiance cloisonnés.
- Une Autorité d'Enregistrement mutualisée sur laquelle peuvent être hébergées des autorités d'enregistrement cloisonnées
- Gestion du cycle de vie des certificats
- Habilitations et rôles d'opérateurs d'enregistrement

- Une interface de type service web sur laquelle peuvent se connecter :
- Une AE hébergée sur votre système d'information
- Un service de personnalisation de supports physiques (cartes, clés USB) en volume ou à l'unité
- Un Back Office complet
- Tout autre système externe pouvant dialoguer sur l'interface

2.4 Audits et référencements

KEYNECTIS s'engage contractuellement auprès de ses clients à leur délivrer un service de certification de qualité alliant performances, disponibilité, fiabilité et sécurité. Ces engagements n'auraient pas de sens si les clients de KEYNECTIS n'avaient pas la possibilité de procéder à des vérifications approfondies du déroulement des services fournis.

C'est pourquoi, dans le cadre d'une démarche Assurance Qualité, KEYNECTIS propose à ses clients de faire réaliser un audit par un professionnel tiers reconnu de la sécurité informatique.

Afin d'accompagner le développement de la certification électronique en France, plusieurs types de référentiels ont été établis. En prestataire expérimenté de la certification, KEYNECTIS accompagne ses clients dans la réalisation de vos projets en conformité avec ces référentiels électroniques parmi lesquels :

2.4.1 Le référencement Minefi[1]

L'objectif de ce référencement est d'homologuer des familles de certificats délivrés par des Autorités de Certification (AC) externes. Les vérifications réalisées dans ce cadre portent sur :

- la conformité à la PC type MINEFI
- la conformité à la réglementation,
- la qualité des services et des certificats.

Les familles de certificats ainsi homologuées sont utilisables par les télé déclarants dans le cadre des télé procédures du MINEFI, par exemple la télé déclaration et le télé paiement de la TVA par les entreprises.

2.4.2 La qualification des prestataires de services de certification électronique

La qualification est selon la Loi, un « *Acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences de particulières de qualités* ».

Démarche volontaire, l'obtention de la qualification est conditionnée à des exigences relatives aux certificats électroniques et aux Autorités de Certification (AC) qui les délivrent. La qualification est une des conditions à remplir pour bénéficier de la présomption de fiabilité d'un procédé de signature électronique

L'Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation, est paru au Journal Officiel le 7 août 2004. Le schéma de qualification, issu des travaux de EGAP a été entériné par le COFRAC dans le courant du premier semestre 2005.

[1] MINEFI : Ministère de l'Economie, des Finances et de l'Industrie

Pour relever le défi des programmes nationaux et européens touchant à l'identité et à la dématérialisation, KEYNECTIS, a passé avec succès, en fin d'année 2005 **le premier audit de qualification PSCE jamais réalisé en France**.

Cet audit, réalisé sous la responsabilité de l'organisme de certification LSTI utilise plusieurs référentiels : au plan européen le document ETSI 101456 v 1.2.1 "Policy requirements for Certificate Authorities issuing qualified certificates" et côté français la norme AFNOR Z74-400 " issue de la traduction du document ETSI, ainsi que l'annexe de l'arrêté du 26 juillet 2004 "spécifications techniques relatives au prestataires de services de certification en vue de la reconnaissance de leur qualification".

Le périmètre audité concerne les services suivants identifiés dans le document ETSI 101456 :

- Gestion du cycle de vie des Autorités de Certification
- Gestion du cycle de vie des certificats qualifiés,
- Gestion du cycle de vie des supports sécurisés de création de signature électronique (SSCD), à savoir personnalisation de supports cartes à puce renfermant les certificats qualifiés, gestion des envois, mailers sécurisés, ….

Les résultats de l'audit ayant été positifs, KEYNECTIS a reçu :

- Le **certificat de conformité** de son système de management à la norme TS101546 (NF Z74 400) pour l'émission de certificats qualifiés au sens de la **directive européenne**,
- Son attestation de conformité par rapport aux exigences de la **réglementation française sur la signature électronique**, ce qui le rend de fait conforme aux exigences nécessaires aux pratiques de signature électronique telles que définies dans la PRISV2 (Politique de Référencement Intersectorielle de Sécurité) de l'ADAE.

2.4.3 La Politique de Référencement Intersectorielle - PRI

Dans le cadre de la modernisation de ses services et de simplification des démarches, le gouvernement procède à la dématérialisation des procédures administratives. L'authentification et la signature électronique à l'aide des certificats électroniques apportent une réponse juste aux questions de sécurité que pose la mise en œuvre de ces télé services.

Pour améliorer la confiance des usagers dans l'Internet, le Gouvernement, au travers de l'ADAE*, a défini et publié la première version d'un document cadre : la PRI - politique de référencement intersectorielle qui vise à identifier quels certificats pour quelles applications entre administrations, administrations et entreprises, administrations et usagers des services publics. Ce document cadre tout en permettant le référencement des familles de certificats, identifie les exigences de contenu et de délivrance des certificats.

**L'ADAE (Agence pour le Développement de l'Administration Electronique) est un service interministériel placé auprès du Premier ministre, mis à la disposition du ministre chargé de la Réforme de l'État. Elle a été créée par le décret du 21 février 2003, publié au JO du 22 février 2003.*

3 L'OFFRE DE KEYNECTIS

L'offre commerciale de KEYNECTIS repose sur la délivrance de certificats numériques (pièces d'identité électroniques) pour instaurer des relations de confiance B to A (Business to Administration), B to B (Business to Business) ou B to C (Business to Consumer). Ce sont des services de certification électroniques en modèle externalisé c'est-à-dire que KEYNECTIS réalise les prestations pour et sur ordre de ses clients.

KEYNECTIS propose donc à ses clients et partenaires de prendre en charge l'ensemble des opérations de fabrication et distribution de certificats.

Le recours à KEYNECTIS doit donc être vu une prestation de sous-traitance où KEYNECTIS intervient en tant que :

- Opérateur de services de certification électronique (fabrication et distribution du certificat électronique depuis son centre d'exploitation)
- Maître d'œuvre sur la mise en place de solutions packagées
- Conseil et assistance à la maîtrise d'ouvrage

Les prestations s'organisent en deux types de services :

- Externalisation de services d'Infrastructures de Clés Publiques (ICP ou PKI) déclinés selon trois niveaux d'engagement :
  - Création et exploitation de services d'enregistrement d'une AC mutualisée
  - Création et exploitation de services de certification sur plate-forme mutualisée
  - Mise en place, supervision et maintenance de plates-formes PKI dédiées
- Mise en place, supervision et maintenance distante de plates-formes PKI sur le site du client (Mode « Ambassade »)

Le principe de cette segmentation est de proposer à chaque organisation une solution évolutive, dimensionnée à la population cible de l'application concernée, de 50 à plusieurs millions d'utilisateurs

Aujourd'hui KEYNECTIS dispose de plusieurs offres personnalisées de services :

K Identity® : Protection des extranets et VPN

- Authentification des utilisateurs nomades
- Authentification de site à site
- Chiffrement des données

K Transaction® : Transactions de confiance

- Signature électronique d'échanges en ligne (contrats, relations clients/fournisseurs, formulaires)
- Horodatage électronique
- Gestion de preuve

K Mail® : Sécurisation de messagerie

- Authentification des expéditeurs, intégrité des messages et confidentialité des échanges
- Génération de clés
- Séquestre et recouvrement de clés

K PKI® : Infrastructure à Clés Publiques générique

- Gestion du cycle de vie des certificats
- Administration des demandes de certificats
- Personnalisation de supports de certificats (cartes à puce, clés USB)

4 REFERENCES CLIENTS (*)

4.1 Secteur public

Dans le cadre de l'opération Télé IR (déclaration et signature en ligne de l'impôt sur le revenu des personnes physiques), la Direction Générale des Impôts a confié à KEYNECTIS, au travers d'un consortium d'intégrateurs retenu par appel d'offres, la mise en œuvre et l'opération d'une Infrastructure de Gestion de Clés (IGC) grand public capable de délivrer des certificats électroniques à l'ensemble des contribuables.

KEYNECTIS a développé pour le Ministère de l'Economie, des Finances et de l'Industrie un processus de distribution et de gestion des certificats électroniques répondant à ses besoins spécifiques, tant en terme d'intégration aux systèmes d'information de la Direction Générale des Impôts (annuaires, bases de données, applications) qu'en terme de disponibilité et de performance du service sur la période très courte précédant la date limite de déclaration des revenus.

Dès la 1ère campagne de télé déclaration (revenus de 2001), KEYNECTIS a généré, en trois semaines, plus de 650 000 certificats.

Sur les 4 dernières années d'exploitation (2002-2005), ce sont plus de 10 millions de certificats électroniques qui ont été générés par KEYNECTIS pour les besoins de la DGI.

Le développement des menaces terroristes et de la fraude identitaire a conduit la communauté internationale à renforcer la sécurité des contrôles aux frontières et donc la fiabilité des documents de voyage.

Dans ce contexte, KEYNECTIS, leader français des services et plates-formes de confiance, a réalisé pour le compte du Ministère de l'Intérieur français la mise en place de la plate-forme de certification pour le passeport électronique français.
Le système installé inclut l'Autorité de Certification française (CSCA), et des robots de signature des passeports (« Document Signer »).

Ainsi, le système fourni par KEYNECTIS permet de gérer l'Autorité de Certification CSCA-FRANCE et les modules de « Document Signer » qui sur le système de personnalisation des passeports électroniques, signent les données sécurisées intégrées dans la puce.

Cette réalisation a permis à KEYNECTIS de démontrer la performance de sa technologie et de son savoir faire en matière de sécurisation des systèmes d'identité (PKI). KEYNECTIS s'est montré très réactif puisque la mise en place aura durée moins de 4 semaines, les premiers passeports électroniques ayant été produits dès le début avril 2006.

Dans le cadre de la sécurisation des échanges électroniques au sein du Ministère de la Défense, la DGA (Délégation Générale pour l'Armement) a confié à KEYNECTIS, au travers d'un consortium d'industriels, la réalisation et la mise en place d'une Infrastructure de Gestion de Clés générique permettant de couvrir des besoins d'authentification, de chiffrement et de signature électronique.

Le Ministère de la Justice a choisi de mettre en place une Infrastructure de Gestion de Clés pour assurer la sécurité des transactions sur son intranet/extranet. Le déploiement concerne l'ensemble des juridictions: système judiciaire, système pénitentiaire ... afin d'accéder de manière sécurisée au fichier des détenus.

Pour une sécurité accrue, le Ministère de la Justice choisit de délivrer les certificats électroniques sur carte à puce.

KEYNECTIS agit en tant qu'opérateur de certification sur l'ensemble du projet et gère le processus complet de fabrication, personnalisation et distribution des supports cartes à puce.

La Poste a décidé de créer son Autorité d'Horodatage, pour répondre :

- d'une part aux besoins de ses propres services électroniques (Lettre Recommandée Electronique)
- d'autre part pour proposer des prestations de tiers horodateur.

KEYNECTIS a mis en place et exploite ainsi une plate-forme capable de produire jusqu'à 120.000 tampons par heure, dans le cadre d'applications postales en premier lieu mais aussi dans l'optique de l'ouverture d'un service commercial de cachets électroniques de La Poste.

4.2 Banques et Assurances

Dans le cadre de la procédure « Télé-TVA », prévue par le Code Général des Impôts (obligatoire pour les entreprises de plus de 15 millions d'euros de CA et facultative pour les autres), menée par le Ministère de l'Economie, des Finances et de l'Industrie (MINEFI), banques et institutionnels se sont positionnés comme Autorités de Certification délivrant des certificats électroniques aux responsables financiers des entreprises, leur permettant l'accès à l'application Télé-TVA (déclaration et règlement de la TVA en ligne). Les besoins de ce projet s'expriment en termes d'authentification, de signature électronique et de confidentialité.

KEYNECTIS assure ici le rôle d'opérateur technique des Autorités de Certification et a développé une architecture d'enregistrement qui s'intègre de façon modulable et progressive dans les structures (siège, directions régionales, agences locales) et systèmes d'informations de ces dernières.

Soumis à des critères très exigeants en terme de délai de réalisation de l'infrastructure et afin que tous ses clients puissent être opérationnels au moment du lancement officiel de la procédure « Télé-TVA », KEYNECTIS a réussi la mise en place du service pour chacun d'eux en moins de trois mois. Dans le même temps, KEYNECTIS les a accompagnés dans la réalisation du dossier de référencement exigé par le MINEFI. Dans son rôle d'opérateur, KEYNECTIS conserve et opère les équipements cryptographiques de ses clients depuis son centre de production.

A ce jour, KEYNECTIS a délivré plus de 80% des certificats électroniques référencés MINEFI (au travers de ses clients institutionnels) soit plus de 80 000 certificats électroniques depuis mai 2001 (date d'ouverture du 1er service Télé-TVA).

GRAS SAVOYE	KEYNECTIS opère l'Infrastructure à Clés Publiques interne et externe de Gras Savoye, 2ème courtier d'assurance français. L'objectif est de sécuriser leur extranet pour faciliter et garantir les échanges avec leurs partenaires.

BNP PARIBAS	BNP Paribas Security Services (BP2S) est la structure de services aux sociétés cotées de BNP PARIBAS. Afin d'offrir à ses clients la possibilité d'utiliser Internet pour «dématérialiser» leurs assemblées générales d'actionnaires, BP2S a souhaité se doter d'une solution de certification électronique. La solution mise en place par KEYNECTIS institue BP2S en Autorité d'Enregistrement. Les données nominatives contrôlées et saisies par BP2S sont transmises sous la forme d'un fichier pour chaque assemblée générale via une interface web par un opérateur central. Les moyens de retrait du certificat électronique sont transmis en retour à BP2S qui les intègre sur son portail : chaque actionnaire obtient ainsi son certificat électronique au travers du portail dédié à son AG, sans requérir d'enregistrement supplémentaire.

4.3 Secteur de la Santé

cpf	Le GIP-CPS est responsable des infrastructures de sécurité liées à la Carte des Professionnels de Santé. L'Infrastructure de Gestion de Clés, opérée depuis plus de deux ans, par KEYNECTIS pour le compte du GIP-CPS a pour objectif de fournir deux profils distincts de certificats serveurs et un profil de certificats de chiffrement pour les utilisateurs sous six Autorités de Certification distinctes. Les demandes d'émission ou de révocation des certificats électroniques sont transmises soit par une interface web soit par un e-mail signé, par le demandeur pour le certificat de chiffrement ou par un opérateur accrédité pour les certificats de serveurs. KEYNECTIS a, en outre, organisé l'intégration complète des services d'enregistrement, de fabrication, de distribution des certificats ; la réalisation, la fourniture et la mise en œuvre des centres d'inscription, du centre d'administration et des outils associés.

4.4 Industrie

AIRBUS	Airbus a développé un portail dénommé AOLS (Airbus On-Line Services) pour ses 200 clients compagnies aériennes et gouvernements à travers le monde, afin de faciliter les échanges d'informations au sein de cette communauté. En particulier, Airbus met à la disposition de ses clients la documentation confidentielle de maintenance des appareils et de réalisation des interventions. Dans ce contexte, Airbus a délégué à KEYNECTIS la mise en place de son infrastructure à clés publiques (gestion des certificats numériques) pour l'authentification et la confidentialité des échanges. En complément de l'opération de l'Autorité de Certification utilisée par AOLS, KEYNECTIS fournit les multiples moyens d'enregistrement des utilisateurs et se charge de la fourniture des supports physiques de certificats électroniques (personnalisation graphique, électrique, codes PIN, logistique des cartes à puce et clés USB, suivi des exportations). A ce jour, l'Infrastructure de confiance AOLS opérée par KEYNECTIS a émis plus de 35 000 certificats dans le monde, tous supports confondus.
Rhodia	Dans le cadre du projet de dématérialisation des échanges au sein du groupe, Rhodia a sollicité KEYNECTIS pour la création et l'opération de son Autorité de Certification. L'infrastructure de gestion de certificats électroniques a permis la mise en place des procédures de signature électronique des ordres comptables entre les centres de frais et la comptabilité centrale.
GS1	La société GS1 fédère l'univers de la grande distribution pour tout ce qui concerne les normes d'échanges d'information. Afin de permettre à ses adhérents d'utiliser en toute confiance les logiciels de type AS2, pour réaliser des échanges EDI sur Internet, GS1 s'est s'institué en Autorité de Certification. Chaque serveur étant susceptible d'utiliser un certificat d'authentification et de signature ainsi qu'un certificat de chiffrement. KEYNECTIS est intervenu auprès de GS1 pour la rédaction d'un guide de bonnes pratiques, a participé à la conception et à la mise en place de l'Autorité de Certification et de l'Autorité d'Enregistrement et en assure le fonctionnement en tant qu'opérateur de certification électronique.
CertiMail	Certimail propose au marché un service de mail certifié reposant sur la constitution d'une preuve électronique de contenu, d'envoi et de réception. La preuve de contenu et d'envoi repose sur la signature à valeur probante de l'émetteur. Les émetteurs doivent donc être dotés de certificats qualifiés de signature électronique afin de bénéficier du premier service de mail certifié à valeur légale. Certimail devient ainsi Autorité de Certification (AC) contrôlant les procédures d'émission, de révocation et de renouvellement des certificats électroniques , tout en externalisant auprès de KEYNECTIS les fonctions techniques de gestion du cycle de vie de ses certificats.

4.5 Communautés de métiers

A la demande de nombreux cabinets contrôlant des OPCVM, la Compagnie Nationale des Commissaires aux Comptes (CNCC) a entrepris le développement d'un dispositif de signature électronique 'commissaires aux comptes' présumée fiable* avec service d'archivage associé.

L'objectif est de mettre en place un processus de dématérialisation des documents (rapport général, attestations, courriers, …) et des échanges à l'attention de ses membres et d'apporter ainsi une présomption de preuve par l'utilisation :

- de certificats dits 'qualifiés' : fournis par l'opérateur de services de confiance, KEYNECTIS, nouvellement créé
- de dispositifs de création de signature électronique sécurisés (cartes à puce certifiées et procédures d'enregistrement face à face)

L'accès au portail CNCC repose sur la fourniture, à chacun des membres, d'un kit de signature électronique permettant d'identifier le signataire d'un document (notion d'authentification) et l'assurant que ce document n'a fait l'objet d'aucune modification durant son transfert ou sa conservation. (Notions d'intégrité et d'archivage).

Pour répondre à cet engagement, KEYNECTIS s'est positionné en 'chef de file', afin de délivrer à la CNCC un service clé en main de création et d'opération de l'Autorité de Certification CNCC.

* répondant aux exigences législatives et réglementaires en vigueur. Le décret du 30 mars 2001 ayant conféré à la signature électronique la même valeur juridique que la signature manuscrite.

** Pour des raisons de confidentialité, certaines de nos références clients ne peuvent être citées.*

5 GLOSSAIRE

Dans ce dossier, certains sigles ou abréviations sont utilisés. Pour la bonne compréhension du texte, voici une liste de ceux qui sont le plus empruntés :

Autorité de Certification (AC)
Egalement appelée Autorité Certifiante (ou Certificate Authority en anglais)
C'est l'entité qui émet des certificats numériques. Elle fixe les modalités liées à la gestion du cycle de vie des certificats (émission, renouvellement, révocation, …). Pour ce faire elle a la charge d'écrire une politique de certification (PC) précisant ces modalités.

Autorité d'Enregistrement (AE)
Entité responsable de l'identification et de l'authentification des demandeurs de certificat électroniques au profit d'une AC, mais qui n'est pas en charge de l'émission des certificats électroniques.

Carte à puce
Support matériel de sécurité dont la puce contient un certificat d'utilisateur et la clé privée associée. Pour activer la puce, il est nécessaire de s'authentifier par utilisation d'un code confidentiel. A la différence du jeton USB qui peut se connecter directement sur le PC de l'utilisateur, la carte à puce nécessite un lecteur spécifique. En revanche, la carte à puce offre une grande surface de personnalisation graphique (ajout du nom et du prénom de l'utilisateur, du logo de la société, …).

Certificat Electronique
Un certificat est un fichier électronique qui représente une pièce d'identité numérique en établissant un lien avec l'entité qui lui est associée. Dans le cas d'un certificat utilisateur, les modalités d'émission d'un certificat (et donc la manière dont le lien entre l'utilisateur et le certificat est réalisé) dépendent de l'Autorité de Certification émettrice de ce certificat. Le certificat utilisateur contient au moins un identifiant li à son utilisateur, la clé publique de l'utilisateur, le nom de l'Autorité de Certification émettrice du certificat, la durée de validité du certificat et un numéro de série. Ce certificat utilisateur est signé par le certificat de l'Autorité de Certification émettrice.

Chiffrement
Opération par laquelle une donnée intelligible est rendue inintelligible afin d'en protéger la confidentialité.

Clé privée
Une clé privée est une clé mathématique gardée secrète par son détenteur. Son usage est de signer électroniquement des données et de déchiffrer celles chiffrées par la clé publique associée.

Clé publique
Une clé publique est une clé mathématique qui peut être rendue publique et dont l'usage est de vérifier les signatures électroniques réalisées par la clé privée associée. Une clé publique peut aussi être utilisée pour chiffrer des données qui sont déchiffrées par la clé privée associée.

Cryptographie
Il existe deux types de cryptographie : la cryptographie symétrique dite à clé secrète et la cryptographie asymétrique dite à clé publique.

Horodatage
Service qui associe de manière sûre un évènement et une heure afin d'établir de manière fiable l'heure à laquelle cet évènement se réalise.

Infrastructure à Clés Publiques (ICP)
Egalement appelée PKI (Public Key Infrastructure) en anglais
Ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

IPSEC
Norme définissant une extension de sécurité pour le protocole IP dans l'objectif d'offrir des services d'authentification, d'intégrité et de confidentialité.

Politique de Certification (PC)
Egalement appelée Certificate Practise Statement (CPS) en anglais. Définit les procédures selon lesquelles les certificats sont générés et gérés. Elle permet de définir le lien de confiance entre l'utilisateur final et le certificat.

Services de Certification (électronique)
Services délivrés par un prestataire de services de certification (électronique)
Ex : délivrance de certificats électroniques, service d'annuaire de certification, fourniture de CRL, fourniture de jeton d'horodatage, archivage...

Signature Electronique
Action de signer des données grâce à un certificat. La signature électronique bénéficie aujourd'hui d'un cadre légal qui permet à la signature électronique d'être reconnue sur le plan juridique au même titre qu'une signature manuelle traditionnelle.

Utilisateur
Désigne les clients et/ou les tiers utilisateurs.