



KEYNECTIS

DOSSIER DE PRESSE



Protecteur d'identité
Protecteur de liberté
dans un monde connecté





Sommaire

1. Fiche d'identité	3
2. Notions de confiance	4
3. Stratégie de services	6
4. Performances et référentiels	10
5. Usages et clients	12
6. Glossaire	14



1. Fiche d'identité

Nom : KEYNECTIS

Date de création : Juillet 2004

Métier :

- Protéger les identités,
- Protéger les données,
- Protéger les échanges entre les hommes au cœur d'un monde connecté.

Mission :

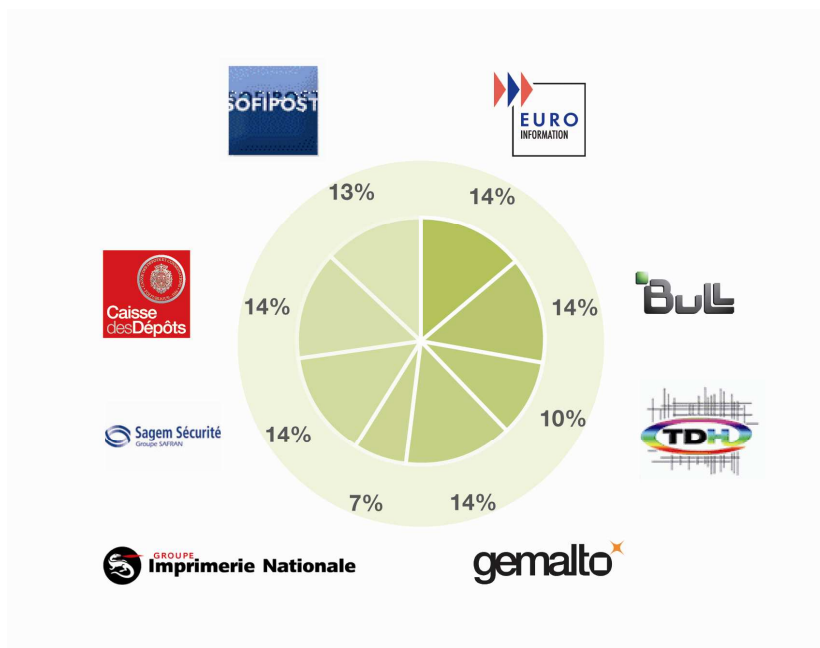
- Favoriser la Reconnaissance et la Confiance entre les hommes,
- Donner à chacun le Pouvoir et la Liberté d'affirmer son Identité,
- Dans tout ce qu'il réalise, à chaque instant, où qu'il soit.

Siège social :

11-13, rue René Jacques – 92131 Issy les Moulineaux Cedex - France
Tel.: +33 (0)1 55 64 22 00 - www.keynectis.com

Nature et répartition du capital social :

KEYNECTIS est porté par un actionnariat fort composé de groupes leaders dans leurs environnements. M. Thierry DASSAULT préside le Conseil d'Administration.





2. Notions de confiance

Les technologies Internet/Intranet ouvrent l'informatique de l'entreprise au monde extérieur, rendant son réseau perméable. Ce faisant, elles accroissent de façon critique les risques de piratage, de destruction et d'espionnage. La sécurité devient de fait une préoccupation majeure - Le danger pouvant venir de l'extérieur comme de l'intérieur des entreprises. De ce fait, la sécurité interne, celle des contenus, occupe une place de plus en plus large dans les problématiques de sécurité.

Par ailleurs la donne change : face à la dématérialisation croissante des échanges, la reconnaissance légale de la signature électronique et le développement des portails d'entreprises qui s'étendent aux partenaires et clients, les entreprises doivent désormais faire face au défi technologique suivant : *faire de leur espace de travail électronique un espace de confiance.*

Dans cette optique, la vocation d'un service de certification électronique consiste à concentrer les services de sécurité requis par les projets de l'entreprise. L'enjeu n'est plus seulement de "sécuriser" le réseau ; il s'agit aussi désormais de « signer », « d'habilitier », de « certifier »...

Parmi les préoccupations majeures des entreprises liées à la sécurité Internet, on compte :

- L'authentification : être sûr de l'identité de la partie avec laquelle vous communiquez
- La confidentialité : chiffrer les données que vous transmettez
- L'autorisation : être sûr que votre interlocuteur est habilité et réciproquement
- L'intégrité : être assuré que les données transmises ne sont pas altérées
- La non répudiation : avoir la preuve que votre interlocuteur a bien reçu votre message et réciproquement

Seule une infrastructure de confiance, appelée communément Infrastructure à Clés Publiques (ICP) ou PKI (Public Key Infrastructure en anglais) répond à l'ensemble de ces besoins en même temps.

Une Infrastructure à Clés Publiques (ICP) repose sur le principe du *chiffrement asymétrique utilisant un jeu de bi-clés* (l'une publique, l'autre privée). Tout le monde peut utiliser la clé publique de quelqu'un pour chiffrer un message car, comme son nom l'indique, cette clé publique a vocation à être distribuée. Mais seul le destinataire du message détient la clé privée capable de le déchiffrer.

Le certificat électronique, véritable pierre angulaire de toute Infrastructure à Clés Publiques, permet d'associer une clé publique à une identité (individu ou système) et est, de fait, à considérer comme un véritable «pièce d'identité électronique».



Schématiquement :

- Dans le monde papier, 2 individus peuvent échanger des informations en toute « confiance » sur présentation respective de leur pièce d'identité
- Dans le monde dématérialisé, 2 individus peuvent échanger des informations en toute « confiance » par l'utilisation d'un certificat électronique

Le certificat électronique est aujourd'hui intégré dans la plupart des grandes initiatives mondiales de modernisation des états par les échanges électroniques pour :

- Le E-Government : le certificat électronique est utilisé comme sésame d'authentification dans les cartes d'identités et les cartes santé, il permet de sécuriser les données des passeports à puce (International Civil Aviation Organization), il sécurise l'accès au dossier personnel fiscal ou santé par Internet, il est normalisé et reconnu pour la signature électronique à valeur probante dans toute l'union européenne, aux US, et la plupart des pays partenaires ont adopté ou sont en cours d'adoption d'un cadre juridique équivalent.
- Les échanges financiers : le certificat électronique est utilisé dans la relation Entreprise – Banque pour le Cash Management, il est à un élément de la sécurité des échanges du réseau financier mondial SWIFT, son implémentation est prévue dans la prochaine génération de cartes bancaires EMV (Eurocard Mastercard Visa).
- Les entreprises : le certificat électronique permet en Europe d'émettre et de transmettre les factures par voie électronique, il est utilisé pour signer des contrats de manière électronique, il est aussi utilisé pour protéger les informations sensibles de l'entreprise (chiffrement des mails, chiffrement des fichiers sur le disque, authentification d'intranets/extranets, sécurisation de paiement en ligne), il permet de mettre en œuvre des réseaux privés virtuels (VPN) grâce au protocole standard IPSec, implémenté par tous les constructeurs d'équipements réseaux.



3. Stratégie de services

Signature électronique

Je signe avec K.Sign® et K.Websign®

Nous communiquons tous de plus en plus, de plus en plus vite. Nous partageons et nous faisons partager de plus en plus d'informations et de créations, professionnelles, confidentielles, contractuelles, officielles et personnelles.

Parce qu'elles nous apportent des gains de temps, de compétitivité, de productivité, les technologies de communication nous sont très vite devenues indispensables. Mais comment signer nos communications, créations et transactions dans l'espace numérique comme nous le faisons depuis toujours dans la vie ? Comment donner au numérique toute la portée et toute la valeur légale que nous savons donner sur le papier ?

KEYNECTIS est aujourd'hui le premier tiers de confiance à avoir lancé un service de signature électronique BtoB et BtoC pour la dématérialisation des flux, documents, contrats, bons de commandes et factures sur le web en mode ASP (Application Service Provider).

En outre, KEYNECTIS dispose d'offres de signature électronique de documents PDF ayant la même valeur légale que les documents papier grâce notamment à l'utilisation d'un outil de vérification de signature gratuit et multilingue disponible dans le monde entier.

- Avec K.Sign® la signature est réalisée sur votre poste de travail à l'aide d'une clé USB (cryptographique) personnelle, qui s'utilise directement à partir du menu outil de bureautique (Adobe® Acrobat®, Microsoft® Office, Open Office, etc.).
- Avec K.Websign® la signature est réalisée par les internautes à distance au travers d'un canal sécurisé. Cette opération ne nécessite aucun pré-requis sur l'ordinateur et fonctionne avec tous les navigateurs du marché.



Identité numérique

Je voyage avec Sequoia® e-passport

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.

Les travaux de l'ICAO (International Civil Aviation Organization), chargée de la normalisation des documents de voyage et des pratiques de production et de vérification associées, ont donné lieu à l'élaboration de spécifications sur lesquelles s'appuient aujourd'hui les industriels pour la mise en place des systèmes de passeport électronique.

- Passeport électronique : Les données du passeport électronique (nom, date de naissance, photo) sont signées électroniquement par l'autorité nationale en employant des méthodes cryptographiques et stockées dans la puce sans contact du document de voyage. Cette procédure, sous contrôle exclusif de l'état, rend le document infalsifiable et authentique. Pendant la lecture d'un passeport électronique, les données sont alors comparées avec celles stockées dans la puce. Ce schéma est également connu sous le terme Basic Access Control (BAC).
- Passeport biométrique : Les données biométriques (empreintes digitales, iris) étant considérés comme sensibles et nécessite une infrastructure protégeant l'accès à ces données. Un lecteur (Inspection System en anglais), doit ainsi s'authentifier auprès du passeport en employant des méthodes cryptographiques. Chaque pays peut alors décider à quel autre pays il souhaite donner le droit de lecture des données biométriques de ses citoyens. Ce schéma est également connu sous le terme Extended Access Control (EAC).

Les passeports électroniques et les passeports biométriques sécurisés par Keynectis offrent aux Gouvernements, aux services de contrôle et de douanes ainsi qu'aux usagers, la meilleure des protections, grâce à la technologie Sequoia® e-Passport.



Authentification

Je m'authentifie avec K.Access®

Dans un monde où nous sommes chaque jour toujours plus nombreux, toujours plus connectés, via plus de canaux, de liens, de flux et d'objets, il est toujours plus indispensable de pouvoir se faire reconnaître, authentifier ses interlocuteurs pour sécuriser les échanges, les dialogues, les transactions. Comment conjuguer liberté, simplicité et sécurité ?

Si la plupart des dispositifs d'authentification forte exige des équipements particuliers à connecter et à transporter, K.Access® permet à un utilisateur de s'authentifier de façon forte en utilisant une clé USB standard ou tout autre support de masse (iPod, téléphone portable, etc.).

Ce support physique est initialisé en utilisant un code d'initialisation confidentiel. Le moyen d'authentification ainsi embarqué est ensuite disponible et protégé par un code PIN. Il peut continuer à être utilisé de façon traditionnelle par exemple pour stocker des photos.

Les utilisateurs peuvent profiter d'une vraie mobilité en introduisant leur clé USB dans tout ordinateur à leur disposition.

Rien n'est laissé sur l'ordinateur après utilisation.



Validation, preuve

Je certifie avec Certify.Center®

A l'heure où les échanges, les messages et les transactions électroniques deviennent de plus en plus stratégiques économiquement, il convient plus que jamais de développer les solutions de certification qui sécurisent les données mais aussi les Hommes.

Mais comment certifier en toute simplicité les milliers de documents administratifs et commerciaux émis chaque jour par nos organisations ? Comment officialiser les documents importants pour être sûrs d'être perçus et entendus parmi des millions de messages électroniques ?

Certify.Center® est une application intelligente, puissante et ultra sécurisée qui gère automatiquement la certification des données et documents transmis, reçus ou archivés.

Avec Certify.Center®, toutes les dimensions de la certification garantissent la sécurité des contenus et favorisent la confiance collective : la signature et la validation sont automatisées, le réflexe sécurité est simplifié.

- Formats de signature Certify.Center® : XADES, XML DSIG, PDF.
- Horodatage : RFC 3161
- Validation OCSP : RFC 2560, CRLv2, http, LDAP
- Certificats électroniques : X509v3, CRLv2

Certify.Center® peut être délivré sous forme de service opéré, de software ou de serveur.



4. Performances et référentiels

Keynectis bénéficie d'un centre de production de type « bunker » **répondant aux plus hautes exigences de sécurité physiques et logiques et assurant la production des certificats électroniques pour le compte de ses clients.**

Au fil du temps, Keynectis a acquis une expertise inégalée en France grâce notamment aux éléments suivants :

- Partage d'expérience avec d'autres opérateurs européens et nord-américains, utilisant certains troncs communs technologiques identiques, permettant de concevoir et d'optimiser les architectures techniques des centres de production, afin d'en renforcer le degré de performance et de maîtriser les montées en charge des besoins clients,
- Confrontation constante aux besoins des grandes entreprises et administrations françaises, aux exigences particulièrement pointues en termes de qualité de services et de temps de réponse,
- Participation systématique aux efforts de structuration et de renforcement du marché, que ce soit par des actions de normalisation, de contribution à la mise en place d'une réglementation adaptée, ou par la conduite de projets innovants au profit de la communauté (projets de type Oppidum par exemple)

Les + du centre

- Site hautement sécurisé incluant contrôle d'accès biométrique et carte à puce, détection d'intrusion et surveillance vidéo
- Infrastructure d'exploitation redondante et secourue
- Suivi unitaire des éléments sensibles (clés cryptographiques, matériels informatiques, principe des secrets partagés et de séparation des rôles, etc.)
- Une équipe multi compétences : R&D, engineering, sécurité, opération
- Habilitation et qualification du personnel 100% dédié à l'opération d'Infrastructure à Clés Publiques
- Une sécurité à l'état de l'art des exigences réglementaires
- Réalisation de veilles technique et juridique sur l'évolution des moyens, des normes et des règlements (PRIS, certificat qualifié).



Basées sur des normes reconnues par l'Etat français et de nombreux gouvernements en Europe et dans le monde, les technologies Keynectis apportent les **garanties de services certifiés par les autorités les plus strictes** :

- Le référencement RGS / PRISV2 : la DGME et la DCSSI, dans le cadre de la sécurisation de la dématérialisation des échanges électroniques entre autorités administratives et usagers (particuliers et professionnels) et entre autorités administratives, ont élaboré conjointement la deuxième version de la Politique de Référencement Intersectorielle de Sécurité (PRIS). L'objet de ce référentiel est de permettre la reconnaissance de produits de sécurité et de prestations de services de confiance pouvant participer à la sécurisation d'échanges dématérialisés.
- La qualification PSCE (Prestataires de Services de Certification Electronique) : Keynectis a obtenu, dans le cadre de son activité d'opérateur de service de confiance, la certification ETSI TS 101 456 (AFNOR Z74 400) et a été le premier prestataire à émettre des certificats qualifiés en France. Les certificats émis aux fins de signature au niveau qualifié signature*** permettent d'obtenir une signature bénéficiant de la présomption de fiabilité, dans le cadre de la directive européenne transposée par l'article 1316-4 du code civil (loi du 13 mars 2000) et le décret du 30 mars 2001 relatif à la signature électronique. Ils correspondent aux travaux normatifs européens de l'ETSI et du CEN, qui traduisent techniquement les exigences de la directive européenne sur les signatures électroniques.
- La certification CC EAL 4+ : La certification selon les Critères Communs fait référence à une méthode reconnue par 22 Etats dans le monde, (dont notamment, la France, les Etats-Unis, la Grande-Bretagne, l'Italie, l'Allemagne, l'Australie, l'Autriche, le Japon,...) permettant de certifier la sécurité de produits et de systèmes de sécurité. Cette certification fournit un haut niveau d'assurance qualité pour les clients de Keynectis et permet aux directions informatiques dans les entreprises de prendre des décisions en toute connaissance de cause quant aux fonctionnalités de sécurité et à la qualité de mise en œuvre de la sécurité au sein de ses produits et services. Le niveau d'évaluation EAL4+ est le plus haut niveau mutuellement reconnu par l'ensemble des pays signataires de l'accord des Critères Communs.
- La certification « Adobe CDS Partner » : Keynectis a été agréé par Adobe pour l'émission de certificats permettant la réalisation et la visualisation universelle de signature électronique de documents PDF.
- CA Browser Forum : En tant qu'Autorité de Certification pour la sécurisation des sites de e-commerce, Keynectis a été référencé dans les navigateurs courants du marché (IE, Mozilla/Firefox, Opéra, Safari)



5. Usages et clients

Keynectis propose une gamme de solutions pour un monde d'utilisations¹

Banques et Assurances

Sécurisation des flux interbancaires, banque de détail à distance, souscription dématérialisée de livret d'épargne, prêt à la consommation, assurance habitation ou automobile, cash management, e-banking, achat en ligne, ...

- AIG
- Allianz
- Amaguiz
- Amaline
- Attijawirafa Bank
- Axa Banque
- Banque Accord
- Banque de France
- Banque des Etats de l'Afrique Centrale
- BNP Paribas
- Boursorama Banque
- Cetelem
- Click & Trust
- CNP Assurances
- Coface
- Cofidis
- Cofinoga
- Crédit Agricole
- Euro Information
- Finaref
- GMF
- Groupama
- HSBC
- Informatique Banques Populaires
- La Banque Postale
- Le Crédit Lyonnais
- Médéric Malakoff
- Monabanq
- Mutualité Française
- Natixis
- Santiane – Groupe Zenith
- Société Générale Corporate Finance
- Sofinco
- Swiss Life
- ...

¹ Liste non exhaustive



Industries & Services

Facture électronique, signature électronique, travail collaboratif sécurisé, traçabilité des identités et des flux, dématérialisation des processus d'approvisionnement, gestion des identités électroniques, sécurisation des e-mails, e-commerce, ...

- Airbus
- Air France
- Areva
- Cardinal Systems
- Carrefour
- EADS
- Eurocopter
- Gemalto
- Informatique CDC
- La Française des Jeux
- Lagardère
- Pixid
- Place Internationale
- Réseau de Transport de l'Electricité
- Sagem Sécurité
- Safran
- Servier
- Thalès
- Valéo
- ...

Secteur Public

Administration électronique, téléprocédures, e-passeport, carte santé, carte d'agent, déclarations sociales et fiscales, marchés publics dématérialisés, immatriculation de véhicules, ...

- Agence de l'Eau Rhin-Meuse
- Agence Nationale des Titres Sécurisés
- ASIP Santé
- ChamberSign
- C^{ie} Nationale des Commissaires aux Comptes
- Conseil d'Etat
- Direction Générale de l'Armement
- Direction Générale des Impôts
- E-Bourgogne
- Imprimerie Nationale
- Ministère de la Défense
- Ministère de l'Economie, de l'Industrie et de l'Emploi
- Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales
- Ministère de l'Intérieur d'Albanie
- Ministère de l'Intérieur d'Algérie
- Ministère de l'Intérieur de Belgique
- Ministère de l'Intérieur du Maroc
- Ministère de l'Intérieur du Qatar
- Ministère de la Justice
- Notaires de France
- RATP
- Registre National des Identités du Guatemala
- Secrétariat Général de la Défense Nationale
- ...



6. Glossaire

Dans ce dossier de presse, 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.

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.

Certificat Electronique qualifié

Il s'agit d'un document sous forme électronique attestant du lien entre les données de vérification de signature (clés cryptographiques publiques) et un signataire, répondant aux exigences de l'article 6 du Décret du 30 mars 2001.

Chiffrement

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

Clé à puce

Support cryptographique physique permettant la fabrication et le stockage sécurisé du certificat électronique. Elle est utilisable sans lecteur, et se connecte sur le port USB de l'ordinateur.

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 s'est réalisé.

Infrastructure à Clés Publiques (ICP)

Egalement appelée IGC (Infrastructure de Gestion de Clés) ou 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 pour les échanges électroniques.

Politique de Certification (PC)

Egalement appelée Certificate Practice 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 porteur du certificat.

Présomption de fiabilité

Les exigences liées à la mise en place d'une signature électronique permettant de bénéficier de la présomption de fiabilité du procédé de signature électronique sont les suivantes :

- La signature électronique met en œuvre une Signature Electronique Sécurisée (SES),
- Cette SES doit être établie grâce à un Dispositif Sécurisé de Création de Signature Electronique (DSCSE),
- La vérification de la Signature Electronique (simple) doit reposer sur l'utilisation d'un certificat électronique qualifié.

Ressource cryptographique

Ressource matérielle stockant des clés privées.

Service 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...



Contact presse :

KEYNECTIS

Caroline DROBINSKI

Tél. : +33 (0)1 55 64 22 85

caroline.drobinski@keynectis.com

www.keynectis.com



*À vous d'imaginer la suite de l'histoire.
Comme toutes vos idées, nous ferons tout pour les protéger.*



© KEYNECTIS Tous droits réservés.