IDNOMIC

# Presentation IDnomic

# SOMMAIRE

# 1 A PROPOS D'IDNOMIC

Dans un monde où les systèmes d'information et les réseaux de communication évoluent sans cesse, où chacun peut accéder à l'information à tout moment quel que soit l'endroit où il se trouve, bénéficier d'un environnement de confiance est primordial.

IDnomic est au cœur des préoccupations des utilisateurs qui veulent communiquer, s'identifier et échanger des informations confidentielles en se sentant protégés :

- Les collaborateurs doivent disposer d'un accès sécurisé aux données de leur entreprise multicanal (postes de travail, ordinateurs portables, Smartphones …), via tout type de réseau et où qu'ils soient (au bureau, dans une filiale ou depuis un point extérieur à l'entreprise).
- Les citoyens ont besoin de documents électroniques d'identité et de voyage lors de leurs déplacements ou pour accéder à un e-service administratif sécurisé.
- Les objets connectés, en pleine expansion, doivent être déployés dans un environnement sécurisé et maitrisé pour être utilisés, en toute confiance, par le grand public.

IDnomic propose son offre en mode Cloud ou licence.

Si la France est la base d'IDnomic et représente 70 % de son chiffre d'affaires avec plus de 200 grands comptes, le monde est également son « terrain de jeux ». La société est présente en Europe, au Moyen-Orient et aux Etats-Unis au travers d'un réseau de partenaires et revendeurs locaux.

IDnomic est ainsi devenu en plus de 10 ans leader européen de la protection et la gestion des identités numériques.

C'est parce qu'IDnomic est un nom fort et impactant qui place l'Humain et la protection de ses identités numériques au cœur de la stratégie de l'entreprise qu'OpenTrust a choisi, début 2016, de changer de nom commercial pour se rebaptiser IDnomic.

# 2 SON ECOSYSTEME

Notre consommation du système d'information a été totalement modifiée avec la généralisation d'internet et des nouveaux modes d'accès au système d'information : l'utilisateur veut pouvoir accéder à l'information à tout moment quel que soit l'endroit où il se trouve.

La banalisation des technologies grand publics (mobile, Wi-Fi, réseaux sociaux, écrans plats, ultraportables, ...) a contraint les entreprises à adopter les technologies dont nous disposons tous à la maison au sein des entreprises : les utilisateurs n'acceptent plus d'être moins bien équipés, dans leurs bureaux qu'ils ne le sont à leur domicile.

L'arrivée de ces technologies grand public incontournables au sein des SI a fait disparaître le périmètre traditionnel du système d'information : le SI s'ouvre à tous les acteurs de l'écosystème et pas aux seuls salariés disposant d'une fiche de paye, il n'y a plus de réseau privé mais un réseau ouvert et peu contrôlable.

Les collaborateurs veulent un accès sécurisé aux données de leur entreprise à partir de toutes sortes d'outils (postes de travail, ordinateurs portables, Smartphones, PDA, poste en libre accès dans un cybercafé etc.), à partir de n'importe quel endroit (au bureau, dans une filiale ou d'un point extérieur à l'entreprise) et via tout type de réseaux (LAN, LS, xDSL, 3G, Wi-Fi, Internet etc.).

L'approche traditionnelle de la sécurité périphérique et la protection classique par identifiants et mots de passe n'est plus aujourd'hui une réponse satisfaisante et les solutions de sécurité périphérique telles que les firewalls et les systèmes de détection des intrusions ne répondent que très partiellement aux nouveaux besoins qui imposent une flexibilité toujours plus grande dans un mode toujours plus complexe à sécuriser.

Pour tirer pleinement profit de ce nouveau 'monde ouvert', les entreprises doivent donc développer des applications de confiance selon lesquelles, il faut être sûre de l'identité de la personne avec qui l'on échange, il faut pouvoir échanger, dans certains cas, en toute confidentialité mais aussi pouvoir signer par exemple un contrat ou une proposition commerciale et enfin être en mesure d'apporter la preuve que l'on a bien envoyé ces documents à l'heure.

La seule réponse technologique capable de satisfaire tous ces besoins de confiance (authentification, confidentialité / chiffrement, intégrité, non-répudiation) de manière transverse est l'infrastructure de confiance, appelée communément Infrastructure à Clés Publiques (ICP), Infrastructure de gestion de Clés (IGC) dans les administrations françaises ou PKI pour Public Key Infrastructure en anglais.

# 3 LA CONFIANCE : SOCLE DE NOTRE METIER

Une PKI 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 une 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 numérique, 2 individus peuvent échanger des informations en toute «confiance» par l'utilisation d'un certificat électronique.

Nous sommes donc aujourd'hui dans une situation ou la technologie peut offrir plus que ce que le marché demande, le véritable enjeu est de diffuser le certificat électronique pour en augmenter l'usage.

IDnomic offre ainsi « out of the box » toutes les fonctionnalités de la confiance numérique intégrée dans une suite logicielle globale et modulaire. Grâce à IDnomic, les utilisateurs accèdent, par exemple, au système d'information de leur entreprise de façon sécurisée via n'importe quel appareil, n'importe quel réseau et à partir de n'importe quel endroit.

De manière simplifiée : en utilisant les logiciels IDnomic on crée de manière transparente pour l'utilisateur une chaîne de confiance basée sur un utilisateur de confiance qui utilise pour se connecter un matériel de confiance via un réseau de confiance à une application de confiance.

Chaque matériel et chaque utilisateur disposent ainsi d'une identité numérique sécurisée qui ne peut en aucun cas être contrefaite. Le système informatique s'appuyant sur cette identité est alors capable d'identifier avec certitude chaque utilisateur/appareil, de déterminer s'il est réputé de confiance ou inconnu et par conséquent de lui autoriser ou non l'accès à certaines ressources.

La « chaîne de confiance » ainsi créée peut être plus ou moins forte selon le degré de confiance de chaque élément de la chaîne donnant accès à plus ou moins de fonctions.

Trois grandes entités interviennent dans la gestion des clés au sein d'une PKI :

- L'Autorité de Certification (AC) : Tiers de confiance faisant autorité pour définir les règles d'attribution et de gestion des certificats (en particulier la définition des éléments et/ou documents à fournir pour prouver l'identité des personnes auxquelles elle délivre les certificats numériques). Pour faire un parallèle avec le monde 'réel', le Ministère de l'Intérieur est Autorité de Certification lorsqu'elle définit les conditions dans lesquelles une carte d'identité ou un permis de conduire doit être délivré.
- L'Autorité d'Enregistrement (AE) : Pour offrir son service de certification, l'AC s'appuie sur une Autorité d'Enregistrement. Celle-ci effectue les contrôles nécessaires, pour tous les demandeurs,

des identités et des attributs demandés sur les certificats (comme l'adresse, la fonction, l'e-mail, etc.). Dans le monde 'réel', l'AE pourrait être une antenne de police, une agence locale de banque ou une mairie.

- L'Opérateur de Services de Certification électronique encore appelé Opérateur de Services de Confiance : 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 (centre de type 'bunker') et un savoir-faire d'exploitation très spécifique, lié à de fortes contraintes sécuritaires. La barrière à l'entrée est donc importante pour émettre le premier certificat électronique et ce constat, qui s'est très vite imposé sur le marché, a conduit à l'émergence du métier de Tiers de Confiance qui mutualise les moyens et les compétences au profit de donneurs d'ordres nombreux (administrations, banques, entreprises privées).

IDnomic est ce Tiers de Confiance. Nous disposons:

- D'une technologie PKI, capable de traiter plusieurs centaines de millions de certificats électroniques et de prendre en compte un grand nombre de donneurs d'ordres avec des exigences de déploiement variées
- D'un savoir-faire opérationnel fruit d'une expérience de plus de 10 ans, qui s'est forgée au cœur des grands projets gouvernementaux ainsi que du monde bancaire et industriel

# 4 NOS PRODUITS ET SERVICES

L'expertise d'IDnomic dans la sécurisation des identités numériques se décline dans 3 grands univers d'utilisation :

- Protection de l'identité numérique des citoyens
- Protection de l'identité numérique des collaborateurs d'entreprise, des terminaux et des machines
- Protection de l'identité numérique des objets communicants

## 4.1 Protection de l'identité numérique des citoyens : Citizen ID

La protection des identités des Nations et de leurs citoyens est un sujet majeur pour tous les gouvernements, ministères, agences ou intégrateurs systèmes en charge de programmes d'identité numérique à grande échelle.

En qualité de partenaire technologique, IDnomic leur propose des solutions leur permettant d'assurer, à leurs citoyens, un maximum de sécurité pour les voyages et les services en ligne comme par exemple :

Des titres d'identité électronique (passeport, titre de séjour, permis de conduire, etc.) non falsifiables

Un accès aux données biométriques sensibles (iris, empreintes digitales) stockées dans les titres sécurisés et une lecture contrôlée des informations

Une production de certificats numériques et une gestion de leur cycle de vie simples et adaptées à des projets à grande échelle.

L'offre Citizen ID est une solution de gestion des identités numériques des passeports électroniques et biométriques, documents de voyages et cartes nationales d'identité électroniques. Conforme aux spécifications de l'OACI et de l'UE et évaluée Critères Communs EAL4+ elle fournit tous les modules nécessaires pour sécuriser la production, la vérification et l'utilisation des titres d'identité électroniques.

Les produits clés de l'offre Citizen ID regroupent :

E-Government Services : Nos solutions peuvent être utilisées seules en tant que modules intégrés dans le système existant de nos clients pour leur permettre d'accéder à des services d'authentification ou de validation de certificat en ligne. Nous pouvons également leur proposer de devenir un Prestataire de Services de Confiance (ou TSP -Trust Service Provider) permettant de gérer totalement les identités numériques de leurs citoyens et de leur fournir les accès nécessaires aux différentes applications gouvernementales.

E-passport : Un projet e-passeport consiste en deux PKI distinctes : une ayant l'objectif de garantir l'authenticité du document (« BAC »), l'autre de protéger l'accès aux données biométriques sensibles (EAC). En s'appuyant sur nos solutions PKI, nous assurons à la fois l'authenticité des titres et la confidentialité des données.

National e-ID : IDnomic propose des solutions permettant d'assurer aux citoyens de bénéficier de titres d'identité électronique (cartes d'identité, titre de séjour, permis de conduire, etc.) non falsifiables par la production de certificats numériques et la gestion de leur cycle de vie pour des projets d'envergure internationale.

## 4.2 Protection de l'identité numérique en entreprise : Corporate ID

L'accélération du développement technologique est accompagnée en parallèle par une cybercriminalité de plus en plus sophistiquée qui menace les infrastructures informatiques des entreprises dans le monde.

Les entreprises doivent ainsi mettre en œuvre rapidement des solutions de sécurité plus abouties pour contrer efficacement ces nouveaux risques d'intrusion et cyber criminalité, afin de protéger leurs informations confidentielles.

Par ailleurs les organisations sont de plus en plus confrontées à la résolution d'une équation complexe alliant flexibilité maximale du système d'information et exigences de sécurité fortes dans un environnement non maitrisé comme par exemple : Comment ouvrir son système d'information à des employés, des partenaires commerciaux, des clients ? Comment utiliser différents types de réseaux (wifi, 3G, VPN, ...) pour accéder au SI ? Comment gérer les identités numériques de mes utilisateurs extérieurs à l'entreprise ? ....

Les DSI/RSSI doivent donc proposer des solutions de sécurisation au sein de leurs entreprises : accès à l'intranet, extranet, serveur, authentification des utilisateurs internes, externes et à distance et les certificats numériques sont un élément de facto standard pour la mise en œuvre de ces solutions de sécurité.

L'offre Corporate ID est une solution ouverte et modulaire qui crée, distribue et gère les identités numériques des utilisateurs ou des terminaux au sein d'une infrastructure de confiance. L'offre Corporate ID s'appuie sur les fonctions de :

OpenTrust PKI : suite logicielle permettant la mise en place d'architectures de confiance fondées sur les standards de la PKI X.509 (Public Key Infrastructure). Développée dans le respect des standards, le produit prend en charge la gestion du cycle de vie des certificats électroniques et des Autorités de Certifications associées. L'approche modulaire de l'architecture d'IDnomic PKI permet une grande flexibilité et facilite la modélisation des PKI les plus complexes.

OpenTrust CMS (Credential Management System) : logiciel complet de gestion du cycle de vie des identités numériques dans un écosystème de confiance. Ses fonctions couvrent toute la suite fonctionnelle nécessaire depuis le bureau des badges jusqu'aux fonctions de self care et help desk pouvant être utilisées sur un très grand nombre d'utilisateurs.

Mobile Guard : permet "over-the-air" de gérer les identités fortes sur Smartphones et tablettes. La suite logicielle permet de créer une chaîne de confiance entre un utilisateur et un Smartphone en assurant une authentification forte du Smartphone et de l'utilisateur.

Virtual Guard : L'authentification par mot de passe, bien que couramment utilisée, ne présente pas toutes les garanties nécessaires pour protéger efficacement les ressources de l'entreprise. Et malgré les avantages incontestés des solutions à base de carte à puce, l'utilisation d'un support physique implique des coûts logistiques qui peuvent être dissuasifs. Avec les cartes à puce virtuelles (Virtual SmartCards) il est possible de bénéficier des fonctionnalités de la carte à puce traditionnelle sans les inconvénients de sa gestion logistique. Virtual Guard - solution complémentaire à la gestion des identités numériques sur cartes et sur mobiles - propose de bénéficier de toutes les fonctions de gestion du cycle de vie des supports cryptographiques appliquées aux cartes à puces virtuelles en utilisant le module TPM (Trusted Platform Module) déjà présent dans la plupart des devices.

## 4.3 Protection de l'identité numérique des objets communicants : Object ID

Internet accueille aujourd'hui des milliards de connexions et d'échanges qui en font l'outil le plus puissant jamais inventé pour le partage de l'information. En quelques décennies, il est devenu le moteur de profondes transformations dans la vie des entreprises, des individus et des institutions.

Après la révolution du smartphone, voici venue celle de l'Internet des objets. Voitures, compteurs d'eau, montres ou électroménager : d'ici à quelques années, la plupart de ces appareils seront connectés au réseau.

Un gigantesque marché se dessine et les estimations vont bon train : entre 25 et 50 milliards d'objets pourraient être connectés d'ici à 2020, pouvant représenter jusqu'à 3.000 milliards de dollars !

La perspective est donc celle d'un monde de connexion hyper dense, entre les hommes mais aussi avec les objets - une connexion permanente et de plus en plus invisible, qui engendre autant de craintes qu'elle est porteuse de promesses.

Nous définissons l'Internet des Objets comme un réseau de réseaux qui permet, via des systèmes d'identification numérique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant.

Mais son développement ne saurait se limiter aux seules questions techniques.

Se pose sous de nouvelles formes, la question des relations entre innovation et marché, entre ressources techniques et applications de services, mais aussi entre sécurité et liberté.

Le poids et l'intérêt économiques de certaines applications contribuent à stimuler les investissements de recherche et développement et à installer durablement les utilisations des objets communicants.

Object ID est une solution de gestion des identités numériques pour les objets connectés. Elle permet la reconnaissance de chaque objet de manière unique, la lutte contre la contrefaçon et le transfert de données à distance pour lancer, le cas échéant, des actions ou pour aider à la prise de décision.

Car tous ces objets sont susceptibles d'envoyer des informations sur leur état, en temps réel ou non, ou d'être sollicités pour effectuer une action : un ordinateur sera mis en veille ou se connectera à un serveur

à distance, la vitesse d'une locomotive contrôlée et diminuée pour raisons de sécurité, l'ouverture d'un pont mobile ordonnée à l'approche d'un bateau …

Le monde automobile, lui aussi, se prépare à une véritable transformation numérique.

Les voitures de demain seront capables de détecter elles-mêmes les dangers sur la route, et de partager l'information avec les autres véhicules, et avec les autorités de sécurité routière.

Le mariage des technologies de l'information et du monde des transports a ainsi donné naissance aux transports intelligents (ITS) et les acteurs du monde automobile rivalisent d'innovation pour renforcer la sécurité et aide à la conduite. Le champ d'application (usages) de cette nouvelle technologie de communication inter-véhicules et avec leur environnement sera très large.

Elle permettra notamment d'alerter/informer le conducteur :

- sur la vitesse maxi recommandée au feu ou sur le temps restant avant le passage au vert
- en cas de véhicules d'urgence en approche : véhicules d'urgence en approche. Il peut ainsi se préparer à leur faciliter le passage sans être pris au dépourvu.
- en cas de travaux sur la chaussée : Les véhicules et équipements lourds de chantier pourront, par exemple, transmettre des données aux véhicules bien avant la zone de travaux.
- en cas de véhicule lent ou d'embouteillage ou en panne sur la chaussée : un signal sera automatiquement envoyé aux autres usagers. La réception anticipée de l'information contribuant ainsi à limiter les risques de mauvaises surprises au volant. De même, le conducteur est alerté en cas d'interruption du trafic ou de bouchon. Les véhicules en aval étant informés d'un arrêt de la circulation en amont, les risques d'accidents sont moindres.
- en cas de mauvaises conditions météo locales : une alerte sur les mauvaises conditions météo locales (forte pluie, chute de neige, chaussées verglacées) est envoyée au conducteur.

Le monde de l'automobile se prépare donc à franchir un nouveau cap en devenant coopératif. Ces facultés additionnelles des véhicules constitueront une évolution majeure et sans précédent à laquelle il faut se préparer dès maintenant. Bref, une petite révolution est en marche … et, pour la mener à bien, ces systèmes communicants auront besoin de sécurité et de confiance numérique par la mise en place d'une infrastructure de confiance (PKI).

Celle-ci permettra de répondre à une problématique de dimensionnement à grande échelle afin d'être en capacité de distribuer des milliards d'identités numériques vers les stations embarquées ITS.

Tel est justement l'enjeu du projet ISE (pour ITS Sécurité), lancé par l'IRT SystemX avec la participation de partenaires industriels tels qu'IDnomic, Renault, PSA Peugeot Citroën, Trialog, Valeo, et d'un partenaire académique, l'Institut Mines-Télécom.

IDnomic participe également au projet SCOOP@F, visant le pré-déploiement national à grande échelle des premiers tests de solutions de communication ITS.

# 5 DELIVRANCE DES SERVICES EN CLOUD OU LICENCE

## 5.1 Le Saas d'IDnomic

Véritable industriel se mettant au service d'une ou de plusieurs Autorités de Certification, IDnomic est un Tiers de Confiance en charge de la fabrication technique du certificat électronique (pièce d'identité électronique) pour le compte et sur l'ordre de l'Autorité de Certification.

Il s'agit d'une prestation industrielle, d'une relation de sous-traitance technique en mode Saas (Software as a Service) également appelé Cloud.

IDnomic opère les PKI des Autorités de Certification qui le souhaitent, et laisse à ces dernières un contrôle total sur les modes d'attribution, de diffusion et d'administration des identités numériques que ces Autorités de confiance délivrent.

Comme tout site industriel, le site de production d'IDnomic situé en Ile-de-France, fait l'objet d'une attention de tous les instants.

Dédié à l'exploitation de services de certification électronique, il se doit d'être à même de tenir compte des évolutions, tant en terme technique, qu'en terme de législation applicable (droit du travail, encadrement des nouvelles technologies …). Les applications de PKI, utilisées par les clients pour gérer leurs certificats électroniques, y sont notamment hébergées.

Pour répondre à ces impératifs, le centre d'exploitation bénéficie de contrôles d'accès biométriques et de plusieurs systèmes de détection d'intrusion avec surveillance vidéo.

Outre ses barrières physiques et logiques, entre 3 et 7 selon les types d'éléments à protéger, la sécurité du service dispose de moyens de redondance aptes à assurer un très haut niveau de disponibilité, ainsi qu'une capacité de reprise d'activité à partir d'un second site d'exploitation informatique.

Un suivi rigoureux et unitaire des éléments sensibles (clés cryptographiques, matériels informatiques, principe des secrets partagés et de séparation des rôles, etc.) est pratiqué par une équipe multi compétences : R&D, engineering, sécurité, opération.

Des moyens de supervision et de remontée d'alerte complètent le dispositif afin d'assurer un contrôle continu et permanent des opérations.

L'ensemble des procédures et des pratiques mises en œuvre pour garantir la sécurité physique et logique de notre centre de production a permis de recevoir de nombreux agréments gouvernementaux et bancaires, gages de qualité et de sérieux pour nos clients.

Grâce notamment à la mutualisation des coûts qu'un Tiers de Confiance peut mettre en œuvre, le mode Cloud ne contient aucun coût caché et permet de très facilement passer d'une application pilote à la généralisation des services de confiance dans l'entreprise.

## 5.2 IDnomic en mode licence

Toutes les entreprises et administrations sont confrontées au même dilemme : Comment améliorer leur compétitivité et leur agilité dans un environnement de plus en plus contraint par la réglementation et par les menaces liées au développement de la cybercriminalité tout en réduisant les coûts ?

Chaque jour de nouveaux utilisateurs ont besoin d'accéder au système d'information tout en protégeant la confidentialité des données. Comment sécuriser les informations vitales de l'entreprise quand, dans une économie où tout se dématérialise, on peut transférer des giga-octets de données vitales en un seul clic de souris ?

Chaque jour de nouveaux devices sont utilisés pour se connecter. Réduction des coûts, satisfaction accrue du personnel, le BYOD procure des avantages indéniables aux entreprises. Comment concilier, dans un environnement sécurisé, mobilité, disponibilité et productivité individuelle ?

Face à ces nouveaux usages, l'approche traditionnelle de la sécurité qui se borne à bloquer l'accès aux utilisateurs non autorisés trouve ici ses limites et ne permet pas d'offrir la flexibilité recherchée.

IDnomic préconise de la compléter par la mise en place d'une infrastructure de confiance en mode licence afin de concilier sécurité et compétitivité.

Ainsi, les logiciels PKI délivrés par IDnomic permettent de déployer rapidement et simplement des solutions de gestion des identités numériques dans un environnement maitrisé.

Grâce à une intégration native avec les logiciels leader d'IAM du marché et au travers de certifications croisées avec nos partenaires, les solutions IDNOMIC offrent une réponse immédiate et sans risque avec un retour sur investissement très rapide.

# 6 AUDITS ET AGREMENTS

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

La qualification PSCE (Prestataires de Services de Certification Electronique) :
IDnomic a obtenu, dans le cadre de son activité d'opérateur de service de confiance, la certification ETSI TS 101 456 (AFNOR Z74 400).

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 d'IDnomic 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.

Le référencement RGS :
L'objectif du référencement RGS est de faciliter les échanges électroniques sécurisés entre les usagers et les autorités administratives mais aussi entre autorités administratives par la mise à disposition d'un catalogue de solutions de sécurité référencées interopérables. Les autorités administratives, dans le cadre de leur migration vers le référentiel RGS, ont obligation d'utiliser des solutions et produits référencés pour leurs systèmes d'information. Ainsi, IDnomic a référencé ses produits afin de proposer ses services et produits pour les plateformes de l'État mais aussi les entreprises souhaitant se connecter à ces plateformes.

La classification Secret OTAN :
La solution CitizenID d'IDnomic a reçu la classification "Secret OTAN" selon le plus haut critère de certification disponible dans le schéma d'évaluation. Figurant au catalogue des produits de sécurité informatique de l'OTAN – NIAPC, catalogue des produits référencés OTAN, CitizenID est la première solution PKI du marché à avoir obtenu un niveau de qualification aussi élevé.

Label France Cybersecurity :
IDnomic s'est vu décerner le label France Cybersécurité pour son offre de protection des objets connectés, Object ID. Le label *France Cybersecurity* vise à faire reconnaître l'offre française en matière de cybersécurité. Il offre la garantie que les produits, solutions et services labellisés sont conçus, développés et opérés en France, par une filière industrielle dynamique et innovante reconnue par le marché. Trois collèges indépendants composés respectivement de représentants des industriels du secteur (ACN, HEXATRUST), des utilisateurs (CESIN, CIGREF, GITSIS, et Espace RSSI du CLUSIF) et des pouvoirs publics (ANSSI, DGA, DGE et Business France) gouvernent le label.

# 7 LES REFERENCES CLIENTS

IDnomic accompagne au quotidien ses clients pour répondre au mieux à leurs problématiques et à leurs besoins. Ainsi les services d'IDnomic s'adaptent à un très grand nombre d'applications métiers.
Pour des raisons de confidentialité, certaines références ne peuvent être citées.

Secteur Public :

Agence Nationale des Titres Sécurisés (ANTS), ASIP Santé, Chambersign, Direction Générale de l'Armement (DGA), Direction Générale des Douanes et des Droites Indirects (DGDDI), Direction Générale des Impôts (DGI), Imprimerie Nationale, Informatique CDC, Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales, Ministère de la Défense, Ministère de la Justice, Ministère du Budget, des Comptes publics et de la Réforme de l'État**,** Notaires de France, Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN).
Projets d'identité nationale parmi lesquels : Albanie, Algérie, Belgique, canada, Chili, France, Gabon, Guatemala, Kosovo, Lesotho, Maroc, Mauritanie, Montenegro, Oman, Ouzbékistan, Qatar, USA, ...

Finance & Assurance :

BNP Paribas, BPCE, Caisse des Dépôts et Consignation (CDC), Euro Information (Groupe Crédit Mutuel), Groupe Crédit Agricole, LCL, Natixis.

Industrie & Services :

ADP, Air France, Airbus, Alstom, Areva, Dassault Aviation, EADS, EDF, Eurocopter, GDF Suez, Gemalto, Kamaz, Michelin, Nissan, RATP, Renault, RTE, Safran, Sanofi, SNCF, SuperValu, Thales, Total, Valéo, Veolia.

# 8 LE RESEAU DE PARTENAIRES

IDnomic dispose d'un réseau de partenaires et revendeurs en France et à l'international :

- Distributeurs & Intégrateurs: Accenture, Adacom, Askon, Alvand Solutions, Arismore, Axiad ID, Bearing Point, BSP, Cap Gemini, Carillon, CGI, Exakis, FISid, Gemalto, Get Group, Giesecke & Devrient, IDpendant, Imprimerie Nationale, NTTcom Security, Oberthur, Orange Business Services, Oxia, Recronet, Safran, Solucom, Sopra-Steria, Synetis, T-Systems.

- Partenaires Technologiques : Airwatch, Cisco, HID, IBM, MobileIron, Oracle, Safenet, Thales, TrustWay, Zenprise.

IDnomic participe également à de nombreux groupes de travail ou est membre de plusieurs fédérations de métiers parmi lesquelles : ACN, Cercle de la Sécurité, Cloud Confidence, Club PSCO, DTCE (Digital Trust and Compliance Europe), EuoCloud, FNTC (Fédération Nationale des Tiers de Confiance), HexaTrust, MEDEF, Syntec Informatique (Syndicat des Sociétés d'Etude et de Conseil) Numérique.

# 9 IDNOMIC EN BREF

Nom commercial : IDnomic est le nom commercial de la société Keynectis

Date de création : Juillet 2004.

Structure capitalistique :
S.A. au capital de 16.026.625 €
IDnomic est porté par un actionnariat fort composé de groupes leaders dans leurs environnements : Gemalto, Morpho (Groupe Safran), Caisse des Dépôts et Consignations, Euro-Information (Groupe Crédit Mutuel-CIC) et TDH (Thierry Dassault Holding).

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

Siège social :
175, rue Jean-Jacques Rousseau – 92138 Issy les Moulineaux Cedex - France
Tel.: +33 (0)1 55 64 22 00 - www.IDnomic.com
https://www.linkedin.com/company/idnomic
Twitter: https://twitter.com/idnomic