



Keynectis-OpenTrust et IBM, partenaires sur le marché des identités de confiance

Aperçu

L'enjeu

Proposer aux entreprises une solution globale et hautement sécurisée de gestion du cycle de vie des identités.

La solution

- Intégration de la suite logicielle Keynectis-OpenTrust à la plateforme IBM Tivoli Identity and Access Manager.
- Offre disponible en mode SOA (Architecture orientée services).

Les bénéfices

- Sécurisation forte des identités et des transactions numériques.
- Contrôle d'accès physique et logique sur un support unique (badge).
- Economies liées à la réduction des appels au Help Desk.
- Mise en œuvre aisée dans la plupart des environnements IT.

Comment contrôler l'accès aux ressources informatiques de l'entreprise avec des smartphones? Comment échanger de façon sécurisée des documents volumineux et confidentiels via Internet? Comment gérer efficacement un très grand nombre d'identités numériques? C'est le métier de Keynectis-OpenTrust, leader européen des solutions et services de confiance, qui s'est rapproché d'IBM dans une relation étroite de partenariat pour apporter une réponse globale et robuste au marché en croissance des identités de confiance.

La suite logicielle de Keynectis-OpenTrust, qui comprend notamment Smart Card Manager (SCM), est à présent intégrée de façon native à IBM Tivoli Identity and Access Manager (IAM). Cette solution complète de gestion des identités s'adresse aux entreprises et aux administrations qui s'engagent dans une gouvernance active de la sécurité.

D'une approche défensive de la sécurité à la confiance

Sherley Brothier, Directeur de la R&D de Keynectis-OpenTrust, analyse l'évolution des stratégies de sécurité dans les entreprises:

«Les entreprises ont longtemps considéré leur système d'information comme un bunker à protéger avec de multiples barrières. Mais les nouveaux modèles informatiques comme le SaaS (Software as a Service), le Cloud Computing et l'accès à Internet par des moyens de plus en plus variés, modifient totalement la donne. Le système d'information s'ouvre aux clients, aux partenaires, aux collaborateurs nomades, souvent au public. Il faut donc adopter une nouvelle approche de la sécurité. Elle repose aujourd'hui sur la confiance.»

D'où la notion d'«identités de confiance» sur laquelle sont fondés les logiciels d'infrastructure de Keynectis-OpenTrust. Les fonctions d'authentification forte, de signature électronique et de non-répudiation permettent d'assurer la sécurité de l'identité numérique de nombreux utilisateurs et dispositifs, à la fois pour les accès physiques et logiques.

De son côté, IBM a élaboré une approche qui formalise les cinq principales exigences de sécurité des entreprises pour limiter l'exposition aux vulnérabilités et aux menaces. La plateforme IBM Tivoli IAM en est l'expression concrète:

- Sécurité physique des infrastructures (bâtiments)
- Neutralisation des menaces au niveau des réseaux, serveurs, postes de travail
- Protection des applications et des process
- Sécurité du capital d'informations et des données
- Gestion des accès et des identités.



«Le système d'information s'ouvre aux clients, aux partenaires, aux collaborateurs nomades, souvent au public. Il faut donc adopter une nouvelle approche de la sécurité. Elle repose aujourd'hui sur la confiance».

– Sherley Brothier,
Directeur de la R&D de Keynectis-OpenTrust.

L'autorité de certification au cœur de la solution

Beaucoup plus performante que la seule gestion des identifications et des mots de passe, inévitablement compliquée et sujette à caution, la solution associant les logiciels Keynectis-OpenTrust et IBM Tivoli IAM est centrée sur le certificat électronique et l'usage d'un support physique unique : les données cryptées (nom du titulaire, limite de validité, autorité de certification émettrice du certificat...) autorisant ou non l'accès à tel bâtiment ou telle application sont stockées sur des cartes à puce (badges, par exemple) ou des clés USB. L'utilisateur n'a plus à faire lui-même la preuve de son identité.

Dans ce système, Keynectis-OpenTrust gère le cycle de vie des identités numériques sur les cartes et tokens, c'est-à-dire le stockage et la mise à jour des certificats sur les supports physiques. L'interface avec IBM Tivoli IAM en fait un système complet et souple avec la gestion des autorisations d'accès (automatisation des contrôles et des mises à jour).

Un univers de confiance performant et pérenne

Ce partenariat entre Keynectis-OpenTrust et IBM est source de plus-value pour les entreprises et les administrations de quelques centaines d'utilisateurs à plusieurs centaines de milliers. Il offre un univers de confiance pérenne alors que les échanges numériques se multiplient et génèrent un besoin croissant de sécurité sur Internet. Ses avantages :

- Une meilleure supervision des accès au système d'information grâce à l'authentification forte et à l'optimisation de la gestion du cycle de vie des identités.
- Une expérience utilisateur positive en raison du support unique, utilisé à la fois pour accéder au bureau, à la cantine et à ses applications.
- Des économies engendrées par une gestion plus pertinente des mots de passe (moins d'appels au Help Desk).

Tous les secteurs d'activité sont concernés : la santé, la finance, l'industrie, la distribution, l'énergie, les collectivités... IBM et Keynectis-OpenTrust mettent leurs offres et leurs compétences à la disposition des organisations qui veulent renforcer la sécurité d'accès à leur système d'information.



© Copyright IBM Corporation 2011

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Tél. : 0810 011 810 - ibm.com/fr

IBM, le logo IBM, sont des marques de International Business Machines Corporation aux Etats-Unis et/ou dans les autres pays. Les autres noms utilisés pour désigner des sociétés, des produits ou des services sont des marques ayant leur titulaire respectif. Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Cela ne signifie pas qu'IBM ait l'intention de les y annoncer. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout élément fonctionnellement équivalent peut être utilisé s'il n'enfreint aucun droit d'IBM. Ce témoignage montre l'utilisation faite par un client d'IBM des technologies/services d'IBM et/ou des Partenaires Commerciaux. De nombreux facteurs ont contribué aux résultats et bénéfices décrits. IBM ne garantit pas des résultats comparables dans tous les cas de figure. Toutes les informations mentionnées ici ont été fournies par le client et/ou par le Partenaire commercial. IBM ne garantit pas l'exactitude de ces informations.

4^{ème} trimestre 2011

© Copyright IBM Corporation 2011 - Tous droits réservés
