Des services de cloud sécurisé pour le gouvernement fédéral grâce à ORC et Entrust

L'exemple de PIVotal ID™ de ORC, une solution d'identification fédérale utilisée par le gouvernement américain, illustre la manière dont l'association d'une solution cloud de gestion des identités en tant que service (IDaaS) et du chiffrement sécurisé peut assurer une forte protection et une grande interopérabilité.

Pour de nombreuses entreprises qui envisagent de transférer leurs données sensibles vers le cloud, la question de sa sécurisation demeure une préoccupation majeure. Mais une entreprise, Operational Research Consultants Inc. (ORC), est en train de démontrer qu'il est effectivement possible de rendre le cloud aussi sécurisé, voire même davantage, que les déploiements sur site, et ce, même pour des organisations aussi exigeantes en matière de sécurité que le gouvernement fédéral des États-Unis.

ORC – UN PIONNIER EN MATIÈRE DE GESTION DES IDENTITÉS FÉDÉRALES

ORC est un partenaire de référence du gouvernement des États-Unis depuis le milieu des années 90 lorsque la société a lancé l'infrastructure à clé publique d'acquisition de la Marine afin de sécuriser les interactions avec les entreprises et les fournisseurs. Alors que le gouvernement mettait l'accent sur la protection des données au cours des deux décennies suivantes, ORC est devenu un partenaire incontournable pour ses solutions de sécurité et l'une des toutes premières entreprises des États-Unis autorisées à fournir des solutions de gestion des identités conformes aux normes gouvernementales.

À ce jour, ORC gère plus de trois millions d'identités et a émis plus de 10 millions de certificats numériques conformes aux normes fédérales à un grand nombre d'employés, d'entreprise, de partenaires, d'anciens combattants et de particulier qui utilisent les services du gouvernement.

ORC

BESOIN DE DISPOSER D'UN SYSTÈME DE GESTION DES IDENTITÉ ET D'AUTHENTIFICATION FIABLE ET INTEROPÉRABLE

En août 2004, l'administration Bush a publié la directive HSPD-12 (Homeland Security Presidential Directive 12) visant à sécuriser les infrastructures et les ressources fédérales en définissant une norme gouvernementale pour garantir la sécurité et la fiabilité des méthodes d'identification. Cette directive va bien au-delà de la simple émission de badges d'identification pour les employés du gouvernement puisqu'elle porte sur les procédures nécessaires à l'émission d'identifiants personnels sécurisés, sur les méthodes de validation de ces procédures et de ces identifiants et sur la gestion du risque et de la qualité tout au long du cycle de vie des identifiants.

Le programme PIV (Personal Identity Verification) est chargé de mettre en œuvre ces procédures, et la norme FIPS (Federal Information Processing Standard) 201 précise l'interface et les éléments de données des carte à puces PIV. Parmi les éléments de données d'une carte PIV figurent une ou plusieurs clés privées de chiffrement asymétriques. Les ministères et les administrations doivent utiliser une infrastructure à clé publique (PKI) conforme en vue de pouvoir émettre des certificats numériques aux utilisateurs. Le programme PIV a également débouché sur le développement d'autres types d'identifications hautement sécurisés qui prennent en charge des interactions spécifiques entre entreprises et administrations, entre particuliers et administrations et entre particuliers et entreprises, lesquels garantissent l'interopérabilité entre les identifications délivrées. Il s'agit notamment de plusieurs variations de la PIV interopérable (PIV-I) et de la PIV, telles que Transportation Worker Identification Credential (TWIC®), First Responder Authentication Credentials (FRAC), Commercial Identity Verification (CIV) et une autorité de certification externe (ECA) PIV-I, qui respectent de nombreuses normes et qui sont développées de manière évolutive. Les procédures et les politiques d'émission de certificats ainsi que les protections accordées à la base critique et aux clés de l'autorité de certification émettrice au sein de cette PKI constituent des éléments essentiels au niveau de protection général du système.

LE DÉFI : MISE EN PLACE D'UN SYSTÈME DE CERTIFICATION INTEROPÉRABLE ET FIABLE

Les systèmes classiques de gestion d'identité sur site sont difficilement transposables sur cloud. Conscient que la sécurité était un élément déterminant pour garantir la fiabilité d'une solution de gestion des identités sur cloud au sein du gouvernement fédéral, ORC savait que disposer d'un chiffrement hautement sécurisé constituait le seul moyen de répondre à toutes les exigences de sécurité du NIST. Dans le cas d'une PKI, cela impliquait que les clés de l'autorité de certification racine et émettrice devraient être générées et protégées au sein d'un matériel hautement sécurisé et certifié FIPS. Au-delà même de la sécurité, il s'agit d'éviter à tout prix que l'une de ces clés ne soit compromise, auquel cas il sera nécessaire de révoquer tous les certificats émis par la PKI et d'émettre à nouveau tous les certificats.

ORC devait en outre respecter plusieurs normes de certification et d'accréditation, dont notamment Federal Bridge, PIV/PIV-I, DoD et FISMA, et être capable de prendre en charge la certification croisée à plusieurs niveaux, ce qui nécessite de disposer d'une solution qui soit en mesure de prendre en charge tout un ensemble de niveaux et de politiques de sécurité. Par ailleurs, la solution devait être éprouvée et reposer sur des normes de systèmes ouverts afin de pouvoir fournir le plus haut degré d'interopérabilité possible. Enfin, il était crucial que ORC puisse disposer de services de chiffrement cloud fiables et hautement sécurisés.

ORC

LA SOLUTION : PIVOTAL ID™ DE ORC ET LES HSM DE ENTRUST

Afin de garantir un haut niveau de sécurité pour les services cloud fédéraux, ORC dispose d'une série de solutions appelées PIVotal ID™. PIVotal ID™ comprend des services gérés certifiés et accrédités permettant d'émettre des certificats d'identification sécurisés fiables dans l'ensemble de l'administration fédérale et capables de se généraliser à l'échelle mondiale, et notamment l'émission de certificats numériques provenant de PKI dont la protection est renforcée par les modules matériels de sécurité (HSM) nShield® de Entrust. ORC émet et gère des millions d'identités conformes qui permettent de sécuriser les opérations des agences fédérales des États-Unis (civiles et défense), de leurs employés, des entreprises internationales, des partenaires commerciaux, des vétérans et des citoyens souhaitant effectuer des démarches auprès du gouvernement des États-Unis et des marchés réglementés. La solution PIVotal ID™ comprend notamment :

- Vérification d'Identification Personnelle (PIV)
- Un émetteur non fédéral interopérable PIV (NFI PIV-I)
- Une autorité de certification externe (ECA)
- Certificats d'accès aux services électroniques (ACES)
- L'autorité de fabrication des certificats TWIC
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

ORC a estimé que la gamme de HSM nShield de Entrust lui permettrait de bénéficier d'une protection et de performances de chiffrement exceptionnelles, ainsi que de la souplesse et l'évolutivité nécessaires pour protéger et gérer les clés racine et toutes les clés sous-jacentes au sein de son infrastructure sécurisée de services cloud.

DES SOLUTIONS OPTIMALES POUR UN CHIFFREMENT FIABLE

Les HSM nShield de Entrust procurent un environnement renforcé et inviolable qui permet de protéger et de gérer les clés confidentielles utilisées pour le chiffrement et la signature numérique en vue de la prise en charge de quasiment toutes les applications allant de la gestion des identités, des services web et du chiffrement des bases de données à la tokenisation, aux services de PKI et à d'authentification forte. Ils constituent le moyen le plus performant d'établir les niveaux adéquats de contrôles physiques et logiques lorsque le degré de protection fourni par le chiffrement logiciel est trop faible.

ORC

LES HSM NSHIELD DE ENTRUST PERMETTENT AUX ORGANISATIONS DE :

- Bénéficier d'une souplesse opérationnelle, d'une disponibilité et d'une évolutivité inégalées pour les environnements cloud et virtualisés.
- Diminuer les coûts de la mise en conformité avec les réglementations en vigueur et des tâches quotidiennes de gestion des clés, telles que la sauvegarde et la gestion à distance.
- Garantir une continuité opérationnelle optimale grâce à un système de gestion des HSM simplifié, une mise à disposition efficace des clés et des fonctionnalités matérielles pleinement résilientes.
- Renforcer la sécurité de vos applications essentielles en protégeant les clés et les opérations de chiffrement au sein d'un matériel inviolable.
- Établir une forte séparation des devoirs et une double vérification au moyen de politiques d'administration rigoureuses, prévoyant notamment une authentification multifactorielle basée sur les rôles et une autorisation basée sur le quorum.

À PROPOS DE ORC

Entreprise du groupe WidePoint et partenaire privilégié du gouvernement fédéral des États-Unis, ORC fournit des solutions de sécurité de l'information aux administrations publiques et aux entreprises afin de leur permettre de garantir des échanges d'informations totalement conformes et fiables. Prestigieux fournisseur de services de sécurité et d'authentification des données entre les entreprises et les administrations publiques, entre les administrations publiques et entre les citoyens et les administrations publiques, les solutions de ORC sont interopérables avec les systèmes existants et s'intègrent parfaitement à toutes les principales applications logicielles du marché. ORC utilise les HSM nShield de Entrust pour fournir des services cloud sécurisés de gestion d'identité au niveau fédéral.

À PROPOS DE ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter:
HSMinfo@entrust.com