Solutions MPKI

L’authentification, l’intégrité et la confidentialité des transactions et des communications sont des aspects critiques, qu’elles se produisent sur Internet, Extranet ou même Intranet. L’infrastructure de sécurité d’une organisation constitue la base de la confiance dans le réseau et constitue la clé de l’authentification, de la vie privée et de la non-répudiation des opérations. S’assurer que les communications sont sûres et que les clients, les employés, les partenaires commerciaux et les consommateurs peuvent communiquer en ligne en toute confiance est devenu essentiel pour les organisations du monde globalisé d’aujourd’hui.

Symantec SSL - Solution Managed PKI (Onsite)

La base de cette solution Managed PKI (Onsite) est sa technologie. Il s’agit d’une plate-forme globale, robuste et de niveau d’entreprise, qui offre à l’organisation le contrôle complet de sa sécurité, de sa confiance, de ses politiques et de son architecture, tout en bénéficiant du savoir-faire et de l’infrastructure de service de Marketware/Symantec SSL.

La solution Onsite offre tous les services de gestion du cycle de vie des certificats, le support d’application et les outils de gestion nécessaires pour exploiter une CA d’entreprise robuste à une petite fraction du coût et de l’effort associé aux solutions "faites-le vous-même" tout en donnant au client un contrôle complet sur les fonctionnalités de l’Autorité d’enregistrement(RA).

Dans cette solution, le client désigne un (ou plusieurs) Administrateur du service Onsite (RA Admin), auquel est attribué un certificat numérique pour accéder au Centre de Contrôle. Cet administrateur aura le contrôle total et exclusif sur tout le cycle de vie des certificats, c’est-à-dire qu’il aura l’autorisation de rejeter, de délivrer, de révoquer et de renouveler tous les certificats numériques.

Hiérarchie: la première étape du processus de mise en œuvre d’une CA consiste à générer la clé de signature racine. La protection de la clé racine est un élément essentiel pour assurer la confiance de l’ensemble de CA. Marketware/Symantec SSL fournit une génération de la clé racine sûre et contrôlée, qui est enregistrée sur cassette et soumise à un notaire pour ne pas répudiation de support.

Une hiérarchie publique est une CA publique, c'est-à-dire que, la hiérarchie est héritée de Symantec SSL. CA publique de Symantec SSL signe la clé racine de CA du client, qui est responsable de la signature de tous les sous-Cas potentiels. Sur tous les certificats, le nom de l'organisation est listé dans CA client. Le client a la possibilité de posséder des clés de sous-Cas supplémentaires. Toutes les sous-Cas sont directement liées à la CA racine du client. Chacune des sous-Cas est gérée indépendamment par le client et fonctionne selon les normes définies pour CA racine.

Ce type de hiérarchie est recommandé si les certificats sont utilisés à la fois dans le système interne du client et à l'extérieur. L'avantage de ce modèle est que tous les certificats ont la capacité de se connecter à la hiérarchie de Symantec SSL et donc de profiter de l'interconnexion de ses clés racine. La distribution de la clé racine de CA est garantie puisque les clés de Symantec SSL font partie intégrante des navigateurs, serveurs et clients de messagerie actuellement utilisés. Par exemple, si un utilisateur envoie un courrier électronique signé à un autre utilisateur possédant un certificat délivré par une organisation au sein de la hiérarchie publique de Marketware/Symantec SSL, cette signature sera automatiquement reconnue comme fiable, du fait qu'elle, est directement liée à une entité extérieure globalement reconnue comme fiable (Symantec SSL).

PKI Architecture: après la création de la hiérarchie, chaque sous-CA est apte à la délivrance et la distribution de certificats numériques à partir de cette PKI d'affaires. La solution Onsite est conçue pour supporter facilement la délivrance de millions de certificats. L'attribution de ces certificats à plusieurs sous-Cas est totalement facultative, mais elle est possible pour la différenciation de certains départements ou projets.

Fonctionnalité: le diagramme suivant montre l'architecture de la solution Onsite de Marketware/Symantec SSL. Les éléments de gauche représentent les utilisateurs, du matériel aux applications client.

Abonnement aux certificats: l'utilisateur se connecte au gestionnaire de souscription, qui est un serveur web géré par CA et utilise les composants Onsite de Marketware/Symantec SSL pour souscrire un certificat. Les demandes de souscription peuvent être approuvées manuellement par les employés de l'organisation assumant les responsabilités opérationnelles du RA, ou automatiquement par comparaison entre les données fournies et celles contenues dans une base de données gérée par l'organisation (Autoadmin).

Les demandes approuvées sont ensuite envoyées (via des connexions sécurisées) à Symantec SSL, où la CA appropriée crée un certificat numérique X.509 v3 et signe la demande. Le certificat est délivré électroniquement à l'organisation par transmission sécurisée. Le même certificat peut être écrit sur un service d'annuaire LDAP, puis remis au client.

Les utilisateurs finaux peuvent utiliser les navigateurs Microsoft, Netscape ou autres pour effectuer leur demande. Les employés ayant des responsabilités administratives peuvent être localisés n'importe où, ce qui permet à l'organisation de répartir les tâches administratives à des endroits éloignés.

Tolérance aux pannes et la récupération Disaster

Le Data Center de Marketware/Symantec SSL assure une disponibilité optimale, i.e. Plusieurs FAI, Pops multiples, UPS et générateurs diesel. En cas de catastrophes naturelles, Symantec SSL possède sur la côte Est des États-Unis un autre Data Center qui peut reprendre le service en 24 heures. Encore plus important est le fait que des simulations trimestrielles de récupération de disaster sont effectuées. La technologie Onsite est basée sur le web, fournissant le support d'un certain nombre de systèmes d'exploitation (NT, Win 2K, Solaris, et HP-UX).

Bon marché

Le coût total de la mise en œuvre et du maintien d'une PKI utilisant la solution Onsite est généralement nettement inférieur à celui d'une PKI entièrement développée et exploitée en interne. Cette réduction du coût total est due à l'absence de besoin de distribution et de maintenance de logiciels propriétaires, la création d'installations de haute sécurité, la compatibilité avec les applications populaires d'affaires et la création d'une récupération de disaster. Toutes ces fonctionnalités sont intégrées dans la solution Onsite.