FICHE TECHNIQUE

Sécurité des appareils mobiles

Intégrez une politique de BYOD et sécurisez les appareils de votre entreprise grâce à la PKI pour appareils mobiles

Une infrastructure PKI (*Public Key Infrastructure*) est une technologie de sécurité reconnue et fiable que les organisations utilisent depuis des décennies pour authentifier les utilisateurs, les machines et les serveurs. Les certificats installés sur les appareils mobiles garantissent que seuls les périphériques et les utilisateurs autorisés peuvent accéder aux ressources de l'entreprise et permettent de sécuriser et de chiffrer les emails sur les mobiles. Ceci permet aux organisations de répondre au désir des employés d'accéder aux e-mails et aux ressources de l'entreprise lorsqu'ils sont en déplacement tout en protégeant les mobiles contre l'accès non autorisé aux applications clés de l'entreprise.

Une seule solution pour les mobiles et les postes de travail

La PKI est une option puissante pour sécuriser tous les terminaux, qu'ils soient mobiles ou de bureau, externes ou internes. Les périphériques eux-mêmes peuvent être identifiés et authentifiés pour empêcher l'accès des machines malveillantes ; les identités d'utilisateurs basées sur le bureau peuvent être transférées sur les périphériques mobiles pour permettre une authentification forte des utilisateurs, ainsi que le chiffrement et la sécurité des e-mails S/MIME. Une solution pour tous les terminaux crée à la fois un environnement sécurisé et convivial pour les utilisateurs finaux et une infrastructure robuste, hautement évolutive et facile à gérer pour les équipes informatiques.

AVANTAGES

- **EMPÊCHER L'ACCÈS DES MACHINES MALVEILLANTES**
  Garantit que seuls les appareils autorisés aient accès aux réseaux et ressources de l'entreprise (par ex. : e-mails, réseaux WiFi, VPN)
- **PRISE EN CHARGE DES APPAREILS MOBILES PERSONNELS ET DU PARC IT**
  Les certificats sont nativement compatibles avec les principaux systèmes d'exploitation mobiles et peuvent être déployés sur les périphériques à l'intérieur ou à l'extérieur du réseau d'entreprise
- **AUTOMATISATION DES DÉPLOIEMENTS**
  Intégrations aux plateformes MDM/EMM pour un provisionnement automatique des identités numériques sur les appareils sans intervention de l'utilisateur final ou d'installation manuelle pour les équipes IT.
- **INTÉGRATIONS MDM/EMM**
  Gestion facilité des certificats en utilisant AirWatch, MobileIron ou le service PKI sur le cloud de GlobalSign
- **FACILE A UTILISER**
  Une fois les certificats installés, les utilisateurs finaux peuvent s'authentifier en toute transparence aux ressources de l'entreprise, ainsi que signer et chiffrer les e-mails
- **INCLUT TOUS LES TERMINAUX**
  Une solution unique pour les terminaux mobiles et les postes de travail simplifie les déploiements et réduit les coûts pour les équipes IT
- **RÉVOCATION DES CERTIFICATS**
  Les équipes IT peuvent révoquer les certificats facilement et à distance en cas de départ de l'employé ou de perte de l'appareil

Sécurité des appareils mobiles

FICHE TECHNIQUE

La solution à 3 problèmes majeurs de sécurité sur les appareils mobiles grâce à la PKI

Sécuriser l'accès des utilisateurs aux ressources et applications de l'entreprise via un appareil mobile

Lorsqu'ils peuvent accéder aux réseaux et aux ressources de leur entreprise à partir de leurs terminaux mobiles, les salariés bénéficient de plus de souplesse pour mener leurs activités, mais protéger cet accès exclusivement à base de mots de passe est insuffisant. Vous devez prendre en considération la mise en place de mesures d'authentification multi-facteurs pour autoriser les accès à partir de périphériques mobiles, comme vous le feriez pour les postes de travail.

L'authentification basée sur les certificats garantit que seuls les utilisateurs autorisés dotés de certificats correctement configurés peuvent accéder aux ressources de l'entreprise à partir de leur appareil mobile. La qualité de l'expérience utilisateur est préservée, avec pour avantage l'absence de clés à gérer ou d'applications d'authentification supplémentaires. Les équipes IT, quant à elles, n'ont plus qu'une seule solution à gérer pour les postes de travail et les terminaux mobiles.

Empêcher l'accès des machines malveillantes

Les réseaux WiFi, les VPNs et systèmes de messagerie sont des points d'accès courants pour toute partie malveillante, qui, une fois l'accès obtenu, peuvent facilement intercepter le trafic et diffuser des logiciels malveillants. Il est crucial de garantir que seuls les périphériques autorisés puissent accèder à vos réseaux et fonctionner sur vos réseaux.

En déployant des certificats aux périphériques mobiles (appareils personnels ou fournis par l'entreprise), vous pouvez identifier et contrôler quels terminaux peuvent accéder à quelles ressources et ainsi aider à empêcher l'accès non autorisé des périphériques malveillants.

Chiffrer et signer les e-mails

Avoir accès à leurs e-mails est généralement la demande la plus courante des employés qui veulent utiliser leurs appareils mobiles au travail. Mais avant que l'accès ne puisse être accordé, des précautions de sécurité doivent être prises, tout comme c'est le cas avec les clients de messagerie pour les postes de travail.

Les certificats S/MIME pour les signatures numériques et le chiffrement des e-mails peuvent être ajoutés aux appareils des employés pour aider à contrecarrer certaines des principales menaces de sécurité et respecter la conformité. Les utilisateurs finaux peuvent facilement chiffrer leurs e-mails pour protéger leur contenu et signer numériquement leurs messages pour prouver leur origine et se différencier des courriels falsifiés.

Automatisez les déploiements grâce à l'intégration aux plateformes MDM et EMM

Les plateformes MDM (*Mobile Device Management*) et EMM (*Enterprise Mobility Management*) facilitent le déploiement de certificats sur les appareils mobiles pour les entreprises. En se connectant directement au service hébergé de certificats de GlobalSign, les organisations peuvent utiliser les plateformes MDM et EMM pour une automatisation complète du provisionnement et de la gestion de certificats. Ceci permet la mise en place d'une politique de BYOD en toute sécurité et empêche tout accès non autorisé. Cette intégration évite aux équipes informatiques d'avoir à installer et gérer manuellement les certificats sur les terminaux de chaque employé. Outre un allègement de la charge administrative, le coût total de possession s'en trouve également réduit.

GlobalSign prend actuellement en charge l'intégration avec

airwatch™ mobile device management

MobileIron (Plateformes Cloud et Core)

A propos de GlobalSign

GlobalSign est un fournisseur leader de solutions de confiance pour la sécurité et la gestion des identités. Au service d'entreprises, de grands groupes, de fournisseurs de services cloud du monde entier et d'innovateurs dans le domaine de l'Internet des objets, GlobalSign permet de sécuriser les communications en ligne, de gérer des millions d'identités numériques vérifiées et d'automatiser les processus d'authentification et de chiffrement. Ses infrastructures PKI de pointe et ses solutions d'identités répondent aux besoins des milliards de services, de terminaux, de personnes et d'objets qui composent l'Internet de Tout.

FR : +9 75 18 32 00
UE : +32 16 89 19 00
RU : +44 1622 766766

ventes@globalsign.com
www.globalsign.fr

GlobalSign GMO INTERNET GROUP