



SecureZIP™

PKWARE®

Les nombreux risques de compromission de données – perte de portable, vol de cassettes de sauvegardes, compromission de serveurs de fichiers – imposent de protéger les données exposées les plus sensibles.

Avec l'augmentation des échanges d'informations au sein de l'entreprise ou avec des partenaires externes, la protection périmétrique du système d'information n'est plus suffisante.

Afin d'assurer l'intégrité et la confidentialité des données, SecureZIP permet le déploiement de solutions de protection efficaces, multiplateformes et simple à utiliser.



SecureZIP : Basé sur des standards reconnus

Les mécanismes de compression de SecureZIP reposent sur le standard ZIP. Cela lui permet d'offrir de fortes performances tout en assurant une facilité de déploiement et une compatibilité vis-à-vis des archives existantes.

Afin d'offrir une protection efficace des données de l'entreprise, SecureZIP incorpore les fonctions cryptographiques de RSA® BSAFE, acteur reconnu de la protection des données. Les protocoles de chiffrement AES et 3DES sont supportés.



Une protection globale

SecureZIP assure la compression, le chiffrement et le transfert des données depuis le poste de travail jusqu'au Mainframe en passant par les différents serveurs et équipements de stockage.

Sur le poste de travail, SecureZIP fournit une interface très simple d'utilisation. En quelques clics, l'utilisateur compresse, signe et chiffre ses données. Un module d'intégration dans Microsoft Outlook ou Lotus Notes offre la possibilité d'en faire de même avec les pièces jointes des e-mails, de manière transparente.

Sur les serveurs et mainframes, les fonctions en lignes de SecureZIP allient compression, chiffrement, signature électronique et gestion des transferts (mail, FTP). Celles-ci s'intègrent dans les scripts batch, la gestion des transferts automatiques ainsi que des sauvegardes.

Sur les équipements de stockages, SecureZIP prend en charge le chiffrement fort et l'intégrité des données, assurant ainsi la conformité à différentes normes et réglementations.

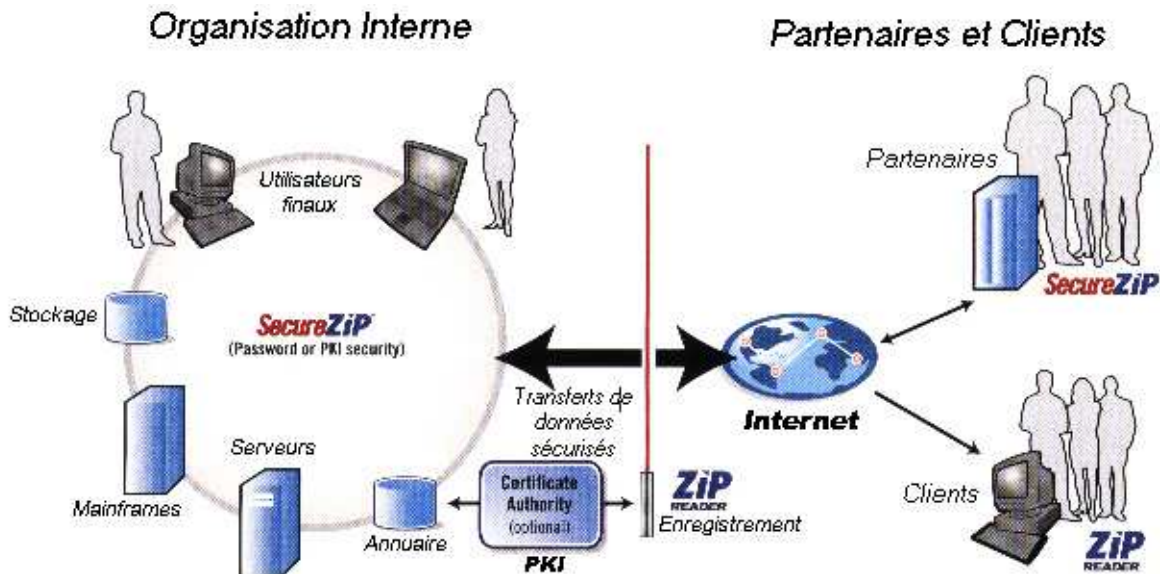


Chiffrement fort et intégrité

Pour une plus grande simplicité, un simple mot de passe peut être choisi afin de chiffrer les données. Cela permet dans la plupart des cas de conserver les informations à l'abri des regards indiscrets.

Pour une sécurité forte, des certificats X.509 peuvent être utilisés. Ceux-ci donnent la possibilité d'un chiffrement fort, ainsi que l'authentification des personnes autorisées à déchiffrer les données.

Les certificats permettent également à un expéditeur de signer électroniquement certaines données et d'en assurer alors l'intégrité et la non répudiation.



Intégration avec une PKI

Lorsque l'utilisation avec certificats est préconisée, SecureZIP peut :

- Soit utiliser une base interne qui regroupe les certificats des différents destinataires choisis,
- Soit s'intégrer avec une infrastructure de gestion de clés publiques (PKI) existante.

Lorsque SecureZIP est intégré à une PKI, la gestion des certificats et des listes de révocations est facilitée.

La mise en place de SecureZIP peut donc étendre le champ d'application d'une PKI existante et en accélérer le retour sur investissement.



Plateformes supportées

- Windows 98, ME, 2000, XP, NT4, VISTA
- Windows Server, UNIX (IBM AIX, SPARC Solaris, HP-UX), Linux
- IBM iSeries (OS/400)
- IBM zSeries (OS-390, z/OS)



Principaux supports physiques d'authentification :

- ActivCard Gold
- Aladdin eToken
- RSA Sign-On Manager
- SafeNet Datakey Axis
- Qvoice WhoIsIt