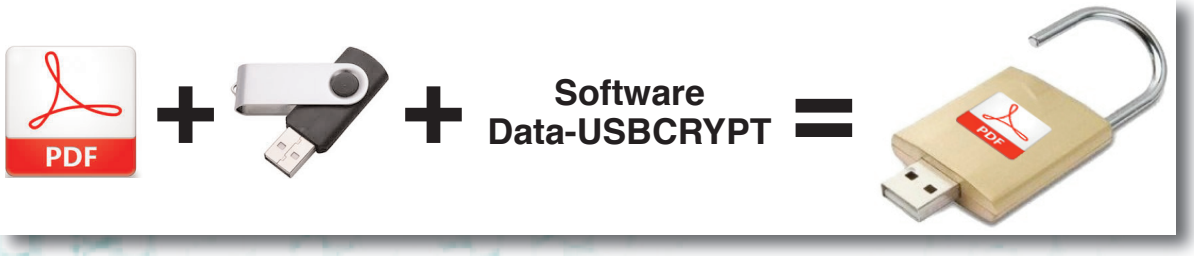
Protection de données par logiciel de cryptage et clé USB standard du commerce ... Grâce au logiciel Data-USBCRYPT©

Etat des lieux :
Il n'existe pas aujourd'hui de solution efficace pour éviter le piratage de documents type PDF.
Ce qui existe vous permet de mettre un mot de passe dans votre document. Mais rien n'empêche l'utilisateur ensuite de communiquer le mot de passe qui permettra d'ouvrir le document. Et donc d'en faire des copies. Même si-celui est crypté.



Logiciel Data-USBCRYPT :
Il à été mis au point le logiciel Data-USBCRYPT une protection de données basée sur le cryptage des fichiers selon le procédé AES-128 associé à une protection d'accès par clé USB standard du commerce. Si vous utilisez toute autre clé que l'originale, le document restera crypté et sa lecture impossible. Cette protection est physiquement liée à la clé à partir de laquelle vous aurez réalisé le cryptage.
Ce principe s'applique, pour le moment, uniquement à des fichiers PDF dont n'importe quel contenu (texte, image, multimédia) pourra être consulté.

Les avantages de ce système sont liés à l'absolue sécurité garantie par le cryptage AES, et le fait que l'accès aux données est autorisée par une clé USB standard du marché. C'est la clé se trouvant connectée qui permettra l'ouverture du document PDF. Vous l'avez compris, vous pouvez si vous le voulez mettre un mot de passe "optionnel" sur le document PDF en protection et parallèlement utiliser la clé qui permettra l'ouverture du document PDF. Le mot de passe pouvant être communiquer en copie la clé physique elle ne pourras pas être copié.

Compatible à partir de Windows XP et sur Macintosh à partir de la version Mac OS X 10.7.
Si vous perdez la clé avec son contenu, l'éventuel mot de passe que vous aurez défini protégera l'accès à vos documents. Si vous vous faites piraté ou avez généré une sauvegarde des données de la clé, il faudra nécessairement que la clé USB se trouve connectée dans l'ordinateur pour ouvrir un document crypté.

Tant que la clé est insérée dans un port USB du Mac ou du PC, et à condition qu'il s'agisse de la clé originale, les fichiers peuvent être décryptés et lus, imprimés (en option), mais ils ne peuvent être ni dupliqués, ni enregistrés, ni enregistrés sous … Il est par contre tout à fait possible de dupliquer les documents cryptés.

Fonctionnement :
Une application dédiée "Éditeur", compatible Mac et PC, assure le traitement préalable des données :
cryptage AES-128 avec le code de votre choix, récupération des paramètres de la clé USB et préparation du fichier de contrôle d'accès (spécifique à la clé USB qui recevra les données). Il convient donc de traiter les clés USB une à une.

Deux solutions existent pour les traitements par lots de grandes quantités de clés :

1) Solution manuelle
- Préparer les données cryptées et les dupliquer sur les clés (les données sont identiques sur toutes les clés),
- Préparer clé par clé, au moment de la vente, le fichier de contrôle d'accès (unique et lié à chaque clé).

2) Solution automatique
Avec le système de duplication de clés USB, le DupliKey©.
Le logiciel de ce système de duplication connecté (compatible PC) est adapté à la sérialisation des clés USB dans le cadre de la protection des données. Il peut donc dupliquer les données et créer le fichier de protection unique à chaque clé.

Évolutions envisagées :
Actuellement dédié aux fichiers PDF, ce principe de protection des données par clé USB standard évoluera vers d'autres types de documents, tels que Word, Excel, images, audio, vidéo et autres. Merci de nous contacter pour répondre à vos besoins.

Avantages :
- Utilisation à moindre coût d'une protection hardware en utilisant une clé USB grand public (que vous trouvez dans le commerce),
- Sécurisation absolue des documents,
- Possibilité de transactions Internet : achat d'un document, d'un livre supplémentaire, mises à jour, protégés par la même clé que possède déjà le client, par l'intermediaire d'une base de donné que vous gérez.

La cible :
Toutes sociétés ayant des données sensibles qui ne doivent pas être copiées. Exemple : les banques, les brevets, données sécurisées d'états et sur un plus large public, les éditeurs de livres, de musiques, photos et vidéos.
Cela permet de donner ou de prêter les sources originales en sachant que la personne ne pourra pas faire de copie décryptée pendant qu'elle possède la clé USB. Photographes professionnels et créateurs d'informations numériques, vous êtes les premiers concernés.

Prix :
Le produit est vendu suivant le nombre de clés que vous désirez protéger. Le logiciel **Data-USBCRYPT©** support de vente se trouve également sur une clé grand public avec verrouillage. Vous pourrez l'utiliser pour :

Pour 25 clés : 12,00 EURO HT
Pour 100 clés : 40,00 EURO HT
Pour 500 clés : 175,00 EURO HT
Pour 1000 clés : 300,00 EURO HT
Pour 2000 clés : 500,00 EURO HT
Pour 5000 clés : 1200,00 EURO HT

Il existe une version de démonstration light, qui permet de crypter 3 documents ou 3 dossiers contenant des PDF et de les associer avec une clé USB.

Dans la version commercialisée, vous disposez des options suivantes :
- Ne pas autoriser d'impression,
- Autoriser l'impression de la page XXX à la page YYY,
- Impression page par page de l'ensemble du document,ou de la page courante uniquement,
- Autoriser toutes les impressions suivant les autorisations du document PDF original,
- Ouverture du document avec mot de passe,
- Autorisation d'ouverture de X jours à partir de la première ouverture,
- Autorisation d'ouverture jusqu'à une date donnée,
- Autorisation d'ouverture de telle date à telle date,
- Autorisation d'ouvertureà partir de telle date,
- Autorisation d'ouverture X fois,

Beaucoup d'autres options encore sont prévues dans les évolutions du produit :
- Si saisie du mot de passe erronnée plus de X fois, destruction du/des documents,
- Blocage des recopies d'écran,
- Screen Saver intégré, pour masquer l'écran après un certain délai d'inactivité, avec mot de passe optionnel pour reprendre la main,
- ...