Pourquoi utiliser XP_CRYPT et SQL Shield?

Le point de vue d'un chef de projet.

1ère partie: DÉFINIR LES BESOINS. Où y a-t-il un manque de protection sur le serveur SQL ?
Protéger les données au niveau champ.
Protéger les procédures de stockage et les scripts.

2ème partie: SOLUTION DE CODE.-Comment protéger efficacement les scripts de protection de code.

3ème partie: SOLUTION DE DONNÉES-Comment augmenter le niveau de protection des données SQL.

4ème partie: DISCUSSION-Achat vs Construction.

1ère partie: DÉFINIR LES BESOINS. Où y a-t-il un manque de protection sur le serveur SQL ?

Protéger les données au niveau champ.

De façon surprenante, le serveur SQL ne crypte pas les données au niveau du champ. L'accès aux données s'effectue en se connectant à la base de données. Mais le fait est que si quelqu'un a accès au système de fichiers, il peut tout simplement copier les fichiers de la base de données, les copier sur un serveur SQL pour lequel il a une autorisation d'administrateur et avoir ainsi accès à l'ensemble de vos données.

Il faut donc en conclure que le système de sécurité du serveur SQL est solide tant que personne n'a accès à votre système de fichiers. Considérant tous les hackers qui sévissent, il faut avoir une confiance incroyable si vous êtes responsable de la protection de données sensibles (comme les cartes de credit, les informations médicales, etc).

Protéger les procédures de stockage et les scripts.

Le serveur SQL permet au développeur de coder de la logique dans la base de données. Cette logique est archivée de la même manière que les procédures stockées, les déclencheurs et les fonctions définies par l'utilisateur. Il y a plusieurs raisons pour lesquelles vous voulez crypter cette logique:

Tout d'abord, les droits de propriété intellectuelle. Si quelqu'un peut voir votre script de logique, c'est exactement comme s'il voyait votre code source. Cela signifie qu'il peut comprendre la logique interne 'secrète' de votre projet, et la procédure de mécanisme inverse est ainsi facilitée.

Ensuite, si quelqu'un peut voir vos procédures stockées, il peut facilement les éditer. Cela signifie qu'il peut réécrire vos procédures stockées et insérer une logique spéciale qui va affecter votre base de données. Quelles sont les conséquences ? Elles incluent l'effacement de données, l'introduction dans votre base de données jusqu'à en arriver à des actes plus sinistres tels que le vol. Sous-entendu écrire ou retrouver des données médicales secrètes, ou créditer un compte bancaire lors d'un achat plutôt que de le débiter.

Beaucoup de développeurs diraient que la plupart de ces données 'devraient' être cryptées au niveau du champ de la base de données. Ces données incluent les numéros de carte bancaire, de sécurité sociale et d'autres informations privées comme les renseignements médicaux.

Cela fait peur n'est-ce pas ? Heureusement, il y a une solution à ces problèmes…

2ème partie: SOLUTION DE CODE. Comment protéger efficacement les scripts de protection de code.

Protéger les scripts….

Ouvrez votre fichier d'aide dans le serveur SQL et vous verrez rapidement que le serveur SQL propose un cryptage pour les procédures stockées et les scripts. Mais avant de pousser un ouf de soulagement, voici ce que le fichier d'aide ne vous dit pas. En 5 minutes, vous pouvez naviguer sur internet et télécharger un des nombreux programmes qui peuvent décrypter en un instant vos procédures archivées 'cryptées par Microsoft'. Cela signifie que n'importe quel pirate digne de ce nom peut entrer dans votre code SQL et faire ce qu'il veut même si vous l'avez crypté en utilisant le cryptage 'originel' des serveurs SQL.

Que pouvez-vous faire ? Heureusement le SQL Shield propose un cryptage de vos procédures stockées qu'aucun programme de piratage connu ne peut décrypter. Ainsi lorsqu'un pirate voit que vos scripts sont cryptés, peu importe combien de fois il utilisera des outils de piratage, il ne pourra pas décrypter votre code de script SQL. Vous êtes donc protégé.

Il devient de plus en plus important de protéger vos données.

3ème partie: SOLUTION DE DONNÉ-Comment augmenter le niveau de protection des données SQL.

Différents algorithmes peuvent être utilisés pour crypter vos données. XP_CRYPT comprend RSA(algorithme asymétrique), AES, Triple DES, DESX et RC4 (algorithmes symétriques). Le choix de l'algorithme dépend de vos besoins.

Notez cependant que les algorithmes asymétriques ont un crypatge relativement lent par rapport aux algorithmes symétriques.

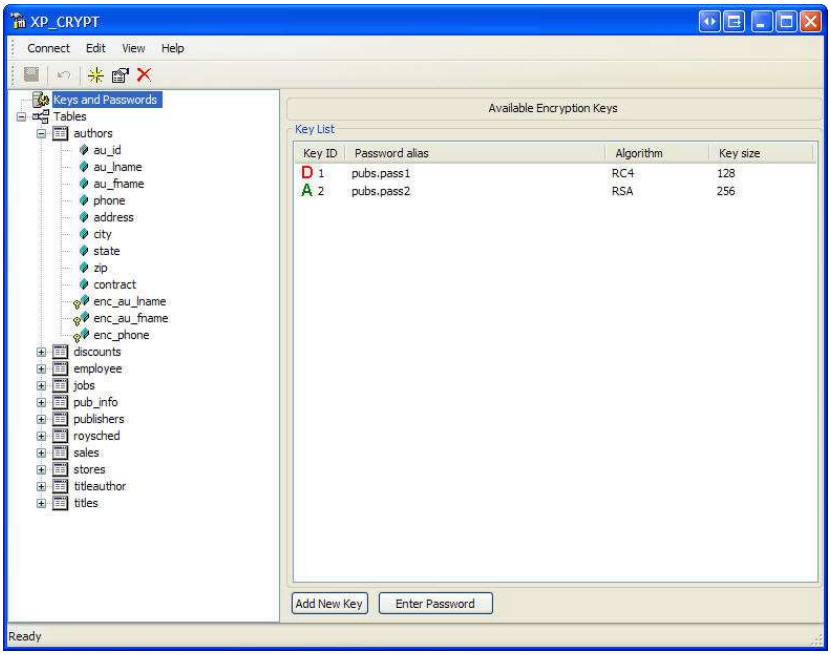
Crypter les champs de données est rapide avec XP_CRYPT en utilisant XP_CRYPT GUI qui est un programme qui introduit facilement des codes de routine dans votre base de données.

XP_CRYPT GUI automatise une somme considérable de travail. Il ajoute tout le code de support et d'interface et l'applique à l'ensemble de votre base de données. Vous pouvez facilement ajouter de nombreux algorithmes avec leur clés respectives. Étant donnés les frais supplémentaires occasionnés par certains des algorithmes les plus puissants, il est plus prudent de proposer différentes sortes de cryptage pour des types de champs différents basés sur la longueur, le type et l'importance du champ.

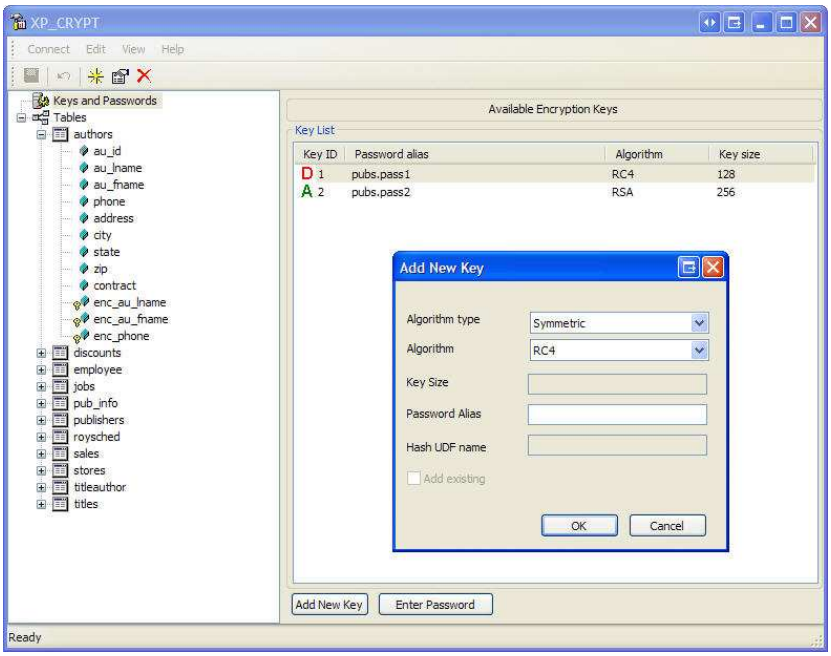
Vous pouvez crypter des champs dans votre base de données en moins de 5 minutes. Le programme exécutera les opérations suivantes:

- 1 Création des tables pour gérer vos mots de passe.
- 2 Création de champs qui sont la représentation cryptée de champs de votre choix (vous effacez les champs sans texte manuellement)
- 3 Création d'une vue qui décryptera les champs que vous avez cryptés.
- 4 Une procédure pour activer et garder la trace de la clé de décryptage pour la session d'utilisateur.

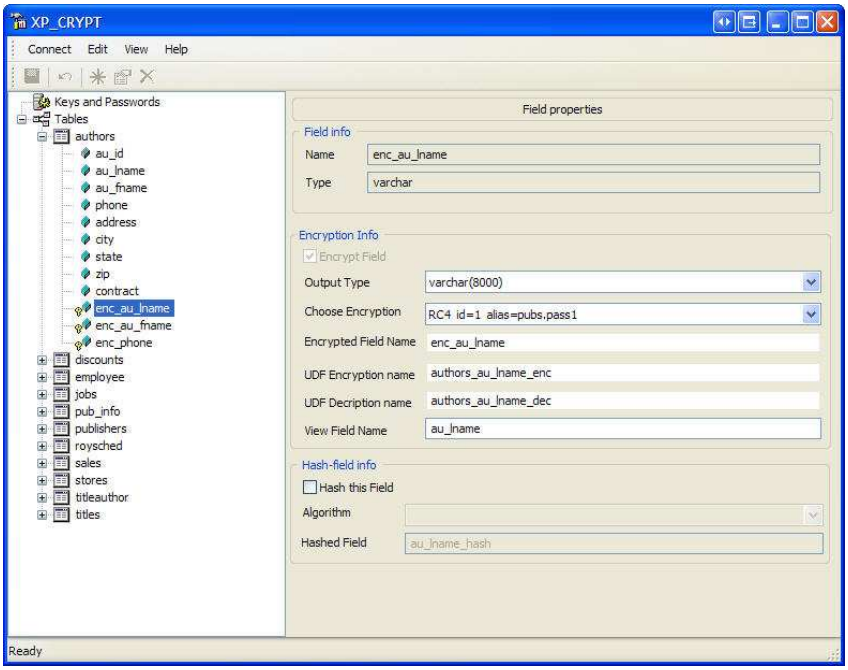
Les images ci-dessous montrent certains des écrans qui sont utilisés pour ajouter un cryptage du nievau de champ à votre base de données.



Vous pouvez ici ajouter plusieurs sortes de cryptage à la base de données en utilisant XP_CRYPT GUI.



Nous pouvons ici définir les caractéristiques d'une clé de cryptage donnée. Différents algoritmes sont pris en charge comprenant des cryptages symétriques et asymétriques.



Nous pouvons ici appliquer les algorithmes de cryptage au(x) champ(s) et choisir le type de sortie et le type de cryptage ainsi que les noms de champs pour les procédures effectuées par XP_CRYPT GUI.

4ème partie: Discussion: Achat vs Construction.

There comes a time when you evaluate a toolkit, when you need to ask the question of buy versus build.

Lors de l'évaluation d'un programme, il y a toujours un moment où l'on compare les avantages et les inconvénients de l'achat et de la construction.

1. Les procédures stockées étendues doivent être **vierges de tout bogue.** Une procédure stockée mal étendue souvent utilisée par la base de données peut corrompre votre base de données. Le fait que XP_CRYPT soit un produit commercial utilisé par de nombreuses personnes réduit ce risque.

2. L'avantage de la construction de votre propre solution est d'avoir le code source. Heureusement, vous pouvez acheter la version de XP_CRYPT **avec le code source.**

3. **Le temps c'est de l'argent**. Construire votre propre programme nécessite beaucoup d'argent si vous voulez avoir plusieurs algorithmes fiables. Grâce à XP_CRYPT GUI, vous allez vite et bien.

4. Combien vaut votre base de données ? Ou plutôt, quel est le pire qui puisse vous arriver si vous perdez l'original de votre base de données ou ne pouvez la décrypter ? Des problèmes comme ceux-ci surviennent avec les bogues. Dépenser plusieurs milliers de dollars pour connaître la tranquilité d'esprit d'une solution reconnue est préférable à se demander si un bogue est niché dans une procédure stockée ou dans le code de cryptage que vous avez écrit vous-même. Si vos **données sont très importantes**, demandez-vous combien cela vous couterait si les choses tournaient mal dans votre base de données.

5. C'est une solution reconnue. XP_CRYPT est déjà utilisé par des organisations gouvernementales, par des entreprises financières, des associations médicales et des universités tout autour du monde.

6. Licence. XP_CRYPT propose de multiples options de licence. **Le prix est très raisonnable** puisque cela n'est qu'une fraction du prix de ses concurrents. Les options de licence comprennent:

a. Licences **uniques** pour un serveur.
b. Licence **de sites** pour couvrir tous les serveurs d'une entreprise.
c. Licence **redistribuable** pour les fabricants de logiciels qui revendent une solution qu'ils veulent protéger. Ils peuvent ainsi offrir leur technologie avec le logiciel.

Lorque vous considérez les avantages et les inconvénients de l'élaboration de votre propre solution, vous vous apercevez rapidement qu'une solution financièrement abordable avec un code source est la meilleure des options. Heureusement, XP_CRYPT est une très bonne solution à un très bon prix.