Crypto-Edition

Spaltenweise AES-256-Bit Verschlüsselung für den Client - unabhängig von der Verschlüsselung der Datenbank - Daten nur auf dem betreffenden Client zu entschlüsseln

Das sichere Verschlüsselungs-Tool für Datenbanken auf dem Client.

Die Besonderheit dieser Verschlüsselung liegt darin, dass die Daten nur auf ausgewählter Hardware und auf dieser nur mit einem Kennwort bzw. nur zugeteilten Chip-Karten entschlüsselt werden können.

Die Daten werden ausschließlich auf den Clients entschlüsselt, der AES-256-Bit Hauptschlüssel ist nicht in der Datenbank und auch nicht auf dem Client gespeichert.

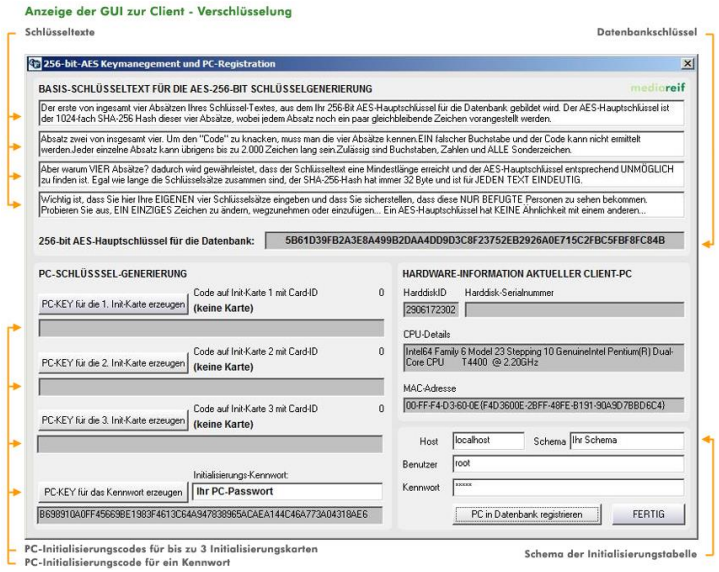
Somit können Datentransfers zum Server nicht „belauscht" werden, da nur verschlüsselte Daten versendet werden. Der Hauptschlüssel wird mit Hardware-Informationen des jeweiligen Clients und Passwort sowie ggf. mit HI. und einem Zugangscode, der auf einer Chip-Karte gespeichert ist, verschlüsselt.

Die Verschlüsselung erfolgt spaltenweise für ausgewählte Spalten, die Daten werden in der Datenbank als verschlüsselte Textfelder gespeichert, es wird also nicht die Verschlüsselung des Datenbank-Systems selbst benutzt. Dadurch wird ein Performance-Verlust vermieden, da der Server die Daten nicht

blockweise entschlüsselt und die entschlüsselten Daten wieder über eine verschlüsselte Verbindung an die Clients senden muss.
Sowohl das Passwort als auch die Chip-Karte muss nur einmal je Systemneustart eingelesen werden. Um Brute-Force-Attacken auf Passwörter zu verhindern, wird nicht das Passwort direkt verwendet, sondern der 1000-fache SHA512-Hash berechnet.

Aufgrund dieser Berechnung können nicht mehr als 10 Paßwörter pro Sekunde ausprobiert werden – ohne dieses Verfahren könnten zig-tausende Versuche pro Sekunde ausgeführt werden.

Dieser Berechnungsvorgang kann nicht abgekürzt werden und bietet somit auch für Passwörter maximale Sicherheit.



Die Crypto-Edition wird vor allem eingesetzt

- Für hochsichere DB-Systeme
- Gegen Datendiebstahl von exponierten Clients
- Health-Care-Daten
- Zutrittskontrollen mit persönlichen Daten z.B. Casino

Features

- schnelle 256-bit AES-Verschlüsselung, unabhängig von Datenbanksystem eigenen Verschlüsselungen
- Wegfall der Datenbanksystem eigenen Verschlüsselung über Benutzername/Kennwort
- Ver- u. Entschlüsselung ausschließlich am Client, keine Serverbelastung, da dieser nicht ganze Tabellen blockweise ver- bzw. entschlüsseln muss
- Einbeziehung von stabilen Hardware-Informationen in die Client-spezifische Verschlüsselung des Hauptschlüssels
- Client/Server-Datentransfer der verschlüsselten und nicht der entschlüsselten Daten, daher keine eigene rechenintensive verschlüsselte Verbindung zwischen Client/Server notwendig
- Ver- u. Entschlüsselung nur auf zugelassenen Clients – Absicherung gegen Datendiebstahl
- Initialisierung der Verschlüsselung je PC mit gleichen oder unterschiedlichen Mifare-Chipkarten je PC bzw. mit einem Kennwort je PC
- Brute-force-Attacken auf das Kennwort durch die ca. 0.1 Sekunden lange Berechnungszeit des finalen Schlüssels extrem erschwert
- Spaltenweise Datenverschlüsselung, für gewünschte Spalten
- Einbeziehung der DatensatzID u. Spaltennamen für die Verschlüsselung
- Manipulationssicherheit von Datensätzen durch verschlüsselten Datensatz-Hash
- Verschlüsselung von Dateien inkl. Dateinamen
- Manipulationssicherheit von Dateien
- Umbenennung von Dateinamen nicht möglich

Crypto Edition

- Erstellen des Hauptschlüssels und der Client-Schlüssel für die Datenbank dank GUI extrem einfach
- Ändern von Initialisierungskarten und Kennworten für jeweilige Clients jederzeit und einfach möglich
- Übersicht über Clients, auf denen ver- bzw. entschlüsselt werden darf, ist immer gegeben, da diese Informationen samt Client-Teilschlüssel in einer Tabelle abgespeichert werden müssen.
- Hauptschlüssel ist nicht in der Datenbank gespeichert, Entschlüsselung des Hauptschlüssels ausschließlich im Arbeitsspeichers des Clients - nur während der Laufzeit der Anwendungen vorhanden
- 100% in C++ geschrieben, daher sehr schnell
- als DLL-Dateien verfügbar, somit in sämtlichen Programmiersprachen einsetzbar
- Verwendung der ODBC - Schnittstelle
- Keine Umstellung Ihrer bereits im Einsatz befindlichen Datenbank
- Keine Auswirkung auf Struktur und Beziehungen Ihrer bereits im Einsatz befindlichen relationalen Datenbank, daher auch kein neues DBMS erforderlich – es fallen keine Kosten für einen Umstieg an
- Kein Mehraufwand für Verschlüsselung, da beim Ver- u. Entschlüsseln nur die Speicher- u. Anzeigefunktion nur um einen Verschlüsseln-JA-Parameter erweitert wird – Zeitersparnis

Erhältlich für folgende Datenbankmanagementsystemen

- Oracle ab Version 8.1
- DB2 ab Version 7
- MySQL ab 4.1
- PostgreSQL ab Version 9.1
- MsSQLServer ab 2000
- Access ab 2003
- SQLite ab 3.6

Systemvoraussetzungen

Intel Pentium ab 500 MHz bzw. gleichwertiger AMD-Prozessor
Arbeitsspeicher: 50 MB
Festplattenplatz: 10 MB
Betriebssysteme: Windows XP, Windows Vista, Windows 7, Windows Server 2000, 2003, 2005, 2008, 2010
Datenbank: Zugangsdaten für Leseberechtigung müssen vorhanden sein.

Hersteller

mediareif Möstl & Reif Kommunikations- und Informationstechnologien OEG
Breitenseer Straße 110/20; A - 1140 Wien
www.mediareif.at
HG. Wien: FN: 215682f; UID-Nr.: ATU 56100203