

Da Häufigkeit und Schwere von Datendiebstahl zunehmen, ist es immens wichtig, dass Unternehmen vertrauliche und sensible Daten zusätzlich durch Verschlüsselung schützen. Ingrian Networks bietet innovative Lösungen, die das Verschlüsseln von Daten praktikabel und kosteneffektiv machen und somit die Risiken bei einem Datendiebstahl oder -verlust eliminieren. Die DataSecure Appliance bietet umfassende Sicherheitsfunktionalität:

- Verschlüsseln kritischer Daten in Web Servern, Application Servern und Datenbanken
- Sorgfältige Kontrolle, Protokollierung und Verwaltung von Datenzugriffen
- Zentralisierte Administration von Zugriff-Policies und kryptografischen Schlüsseln

DataSecure integriert sich nahtlos in das Datenbanksystem und unterstützt unter anderem DB2, Oracle und SQL Server; die Verschlüsselung der Daten erfolgt auf Spaltenebene. DataSecure rationalisiert den administrativen Aufwand, der in der Regel mit Datenbankverschlüsselung verbunden ist - der gesamte Implementierungsprozess ist automatisiert und ermöglicht eine Integration ohne nennenswerte Störung des produktiven Betriebs.

Die DataSecure Plattform besteht aus drei Komponenten:

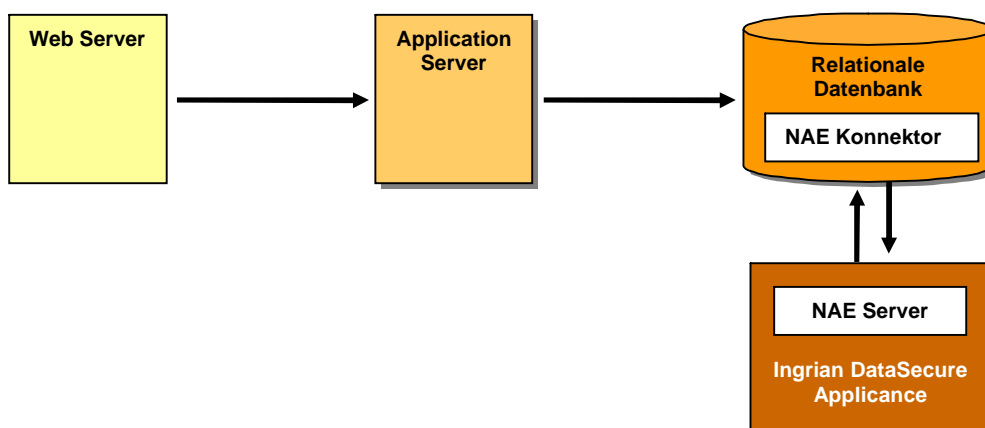
- Die DataSecure Appliance - ein dediziertes, gesichertes Hardware System
- Der Network Attached Encryption™ (NAE) Server (auf der DataSecure Appliance)
- Der NAE Konnektor - Installiert auf dem Web, Application oder Datenbank Server.

Die Integration der DataSecure Appliance in eine existierende Datenbankinfrastruktur ist einfach und schnell zu bewerkstelligen. Für die Network Attached Encryption wird der so genannte NAE Konnektor bei der Installation auf dem Datenbankserver aktiviert und verbindet die Datenbank mit dem NAE Server auf der DataSecure Appliance.

Das webbasierte User Interface auf DataSecure, die Management Konsole, führt Schritt für Schritt durch den Verschlüsselungsprozess für die ausgewählten Tabellenspalten. Der NAE Konnektor auf der Datenbank generiert alle notwendigen Stored Procedures und Funktionen:

- Encryption und Decryption innerhalb der Datenbank
- Migration lesbarer Daten in Ciphertext und Erweiterung des Datenbankschemas um verschlüsselte Spalten
- Periodischer Wechsel kryptografischer Schlüssel (Key Rotation)
- Automatisierung nachfolgender Verschlüsselungsoperationen
- zusätzliche Authentifizierung durch separate Berechtigungen

Diese transparente Integration bedeutet, dass SQL Syntax im Normalfall nicht angepasst werden muss und dass, noch wichtiger, keine zusätzliche Logik für kryptografische Operationen entwickelt werden muss. Eine zusätzliche Authentifizierung sorgt dafür, dass nur über DataSecure definierte Benutzer Dateneinsicht erlangen; selbst Systemadministratoren mit hohen Privilegien können ohne DataSecure Berechtigung nur Daten in verschlüsselter Form selektieren. Das folgende High-Level Diagramm zeigt den Einsatz der DataSecure Lösung:



Das Diagramm verdeutlicht, wie ein Webserver über einen Application Server auf sensible Daten in einer Datenbank zugreift. Der NAE Konnektor ist auf der Datenbank installiert und vertrauliche Daten sind in verschlüsselter Form gespeichert. Der Benutzer, der die Abfrage tätigt, muss verschiedene Berechtigungen besitzen:

- Userid für die Datenbank
- Zugriffserlaubnis für den Schlüssel auf DataSecure

Ist eine der beiden Bedingungen nicht gegeben, wird ein Zugriff nicht erlaubt. Im anderen Fall liefert der NAE Server auf DataSecure die entschlüsselten Daten zurück an die Datenbank-Schnittstelle.

Die kryptografischen Operationen werden auf der DataSecure Appliance durchgeführt, sowohl der NAE Server als auch die kryptografischen Schlüssel liegen auf diesem in sich geschlossenen Sicherheitssystem.

Wie werden Daten verschlüsselt?

Vor der Implementierung einer DataSecure Appliance sind sensible Daten aller Wahrscheinlichkeit nach in lesbarer Form gespeichert; die logische Frage ist also: Wie werden lesbare Daten in ein verschlüsseltes Format migriert? Dieser Prozess ist einfach und überschaubar und über das GUI der Appliance automatisiert.

Nachdem die zu verschlüsselnden Daten identifiziert sind, wird DataSecure für den automatischen Migrationsprozess konfiguriert. Dies beinhaltet die Verbindung zur Datenbank(einmalig) sowie die per Click durchzuführende Übernahme von Tabellen- und Spaltenmetadaten(iterativ).

Um die Einfachheit dieses Prozesses zu beschreiben, dient die Kontonummer in einer Tabelle KUNDEN als Beispiel; diese Spalte KONTONR soll nun verschlüsselt werden. In einem ersten Schritt benennt DataSecure die Tabelle in KUNDEN_ENC um. Dies ist nötig, weil später eine View mit dem Namen der ursprünglichen Tabelle erzeugt wird.

KUNDEN				
KUNDENNR	NAME	EMAIL	KONTONR	BLZ
101	Heiner Müller	H.Mueller@clearnote.de	111222333	50780032
102	Gerhard Ritter	Ritter.G@clernte.net	555666777	40188734
103	Gabi Schneider	gschneider@larnot.de	123456789	51100256

KUNDEN_ENC				
KUNDENNR	NAME	EMAIL	KONTONR	BLZ
101	Heiner Müller	H.Mueller@clearnote.de	111222333	50780032
102	Gerhard Ritter	Ritter.G@clernte.net	555666777	40188734
103	Gabi Schneider	gschneider@larnot.de	123456789	51100256

Im nächsten Schritt legt der NAE Server der DataSecure Appliance eine temporäre Tabelle an, die die ausgewählte(n) Spalte(n) enthält und automatisch eine ROW-ID hinzufügt, welche später für die Rückgabe der verschlüsselten Werte an die Tabelle genutzt wird. Gleichzeitig werden die Werte in der Spalte KONTONR auf NULL gesetzt.

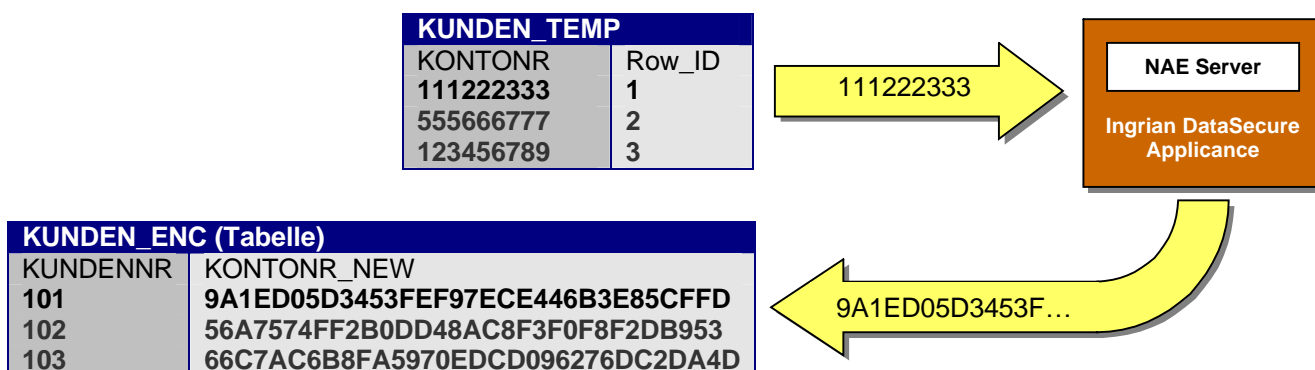
KUNDEN_ENC				
KUNDENNR	NAME	EMAIL	KONTONR	BLZ
101	Heiner Müller	H.Mueller@clearnote.de	NULL	50780032
102	Gerhard Ritter	Ritter.G@clearnote.net	NULL	40188734
103	Gabi Schneider	gschneider@larnot.de	NULL	51100256

KUNDEN_TEMP	
KONTONR	Row_ID
111222333	1
555666777	2
123456789	3

Bevor die Verschlüsselung beginnen kann, fügt DataSecure eine neue Spalte KONTONR_NEW als binären Datentyp ein. Die Länge ist dabei abhängig vom Verschlüsselungsalgorithmus und wird automatisch berechnet; verschlüsselte Daten im Binärformat benötigen mehr Platz als lesbare alphanumerische oder numerische Formate, daher beträgt die Länge nun 16 Bytes. Das Beispiel nutzt einen AES 128-Bit Cipher mit EBC mode.

KUNDEN_ENC Schema			KUNDEN_ENC Schema		
Spaltenname	Datentyp	Länge	Spaltenname	Datentyp	Länge
KUNDENNR	NUMBER	5	KUNDENNR	NUMBER	5
NAME	VARCHAR	20	NAME	VARCHAR	20
EMAIL	VARCHAR	25	EMAIL	VARCHAR	25
KONTONR	CHAR	10	KONTONR	VARBINARY	16

Sobald die neue Spalte hinzugefügt wurde, können die Daten migriert werden. Bevor die Kontonummern nun in die Tabelle KUNDEN_ENC zurückgeschrieben werden, sendet der NAE Konnektor auf der Datenbank die Werte aus der temporären KUNDEN_TEMP Tabelle an den NAE Server, der dann die Inhalte verschlüsselt und an den NAE Konnektor zurückgibt, der diese wiederum in der Tabelle KUNDEN_ENC einfügt.



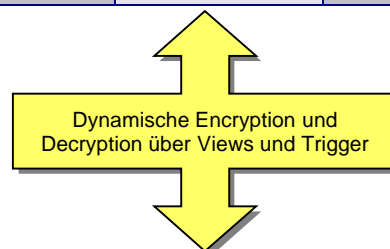
Nach erfolgter Verschlüsselung wird die temporäre Tabelle KUNDEN_TEMP gelöscht; die Tabelle KUNDEN_ENC enthält nun die verschlüsselte Kontonummer. Der Ciphertext in KONTONR_NEW wird in Base64 dargestellt, 32 Zeichen repräsentieren 16 Bytes Binärdaten:

KUNDEN_ENC			
KUNDENNR	NAME	EMAIL	KONTONR_NEW
101	Heiner Müller	H.Mueller@clearnote.de	9A1ED05D3453FEF97ECE446B3E85CFFD
102	Gerhard Ritter	Ritter.G@clernte.net	56A7574FF2B0DD48AC8F3F0F8F2DB953
103	Gabi Schneider	gschneider@larnot.de	66C7AC6B8FA5970EDCD096276DC2DA4D

Wie wird die Verschlüsselung automatisiert?

Nach erfolgter Tabellenmigration erzeugt DataSecure Views, Trigger und Stored Procedures über den NAE Konnektor. Auf diese Weise können Applikationen ohne Änderung Abfragen und Updates auf die modifizierte Tabelle durchführen; in diesem Beispiel generiert DataSecure die View KUNDEN, die dann unverschlüsselte Werte an die Anwendungen zurückliefert oder neue Einträge verschlüsselt:

KUNDEN_ENC (View)				
KUNDENNR	NAME	EMAIL	KONTONR	BLZ
101	Heiner Müller	H.Mueller@clearnote.de	111222333	50780032
102	Gerhard Ritter	Ritter.G@clernte.net	555666777	40188734
103	Gabi Schneider	gschneider@larnot.de	123456789	51100256



KUNDEN_ENC (Tabelle)			
KUNDENNR	NAME	EMAIL	KONTONR_NEW
101	Heiner Müller	H.Mueller@clearnote.de	9A1ED05D3453FEF97ECE446B3E85CFFD
102	Gerhard Ritter	Ritter.G@clernte.net	56A7574FF2B0DD48AC8F3F0F8F2DB953
103	Gabi Schneider	gschneider@larnot.de	66C7AC6B8FA5970EDCD096276DC2DA4D

Wie zu erkennen ist, hat die View den gleichen Namen wie die Ursprungstabelle KUNDEN, daher funktionieren weiterhin auch alle SQL Statements, die die nun verschlüsselten Daten referenzieren. Ebenso fangen Trigger alle auf die View stattfindenden Inserts und Updates ab und sorgen für eine Verschlüsselung über die DataSecure Appliance vor Einfügung in die Datenbank.

Zusammenfassung

Wie bereits dargestellt, ist die Verschlüsselung sensibler Daten über den Datenbank-NAE Konnektor der DataSecure Appliance ein simpler und schnell durchführbarer Prozess, der durch Generierung von Views, Triggern und Stored Procedures komplettiert wird. Sehr wichtig dabei ist, dass die Integration von DataSecure vollständig transparent für alle Anwendungen ist, die auf die verschlüsselten Daten zugreifen müssen. Über die Management Konsole der DataSecure Appliance ist der gesamte Prozess automatisiert, hier werden auch die genutzten Schlüssel und Berechtigungen verwaltet.

Ingrian i221 Management Console
Clearnote-i221 [Logout gschil](#)

Database Table Properties

Column Encryption for Table KUNDEN [Help](#)

Items per page: 10

Column Name	Type	Width	Encryption	Key	Attributes
<input checked="" type="checkbox"/> KUNDENNR	NUMBER	5	None		unique, index
<input type="checkbox"/> NAME	VARCHAR2	20	None		
<input type="checkbox"/> EMAIL	VARCHAR2	25	None		
<input type="checkbox"/> KONTONR	VARCHAR2	10	AES	ingrian_example_key	
<input type="checkbox"/> BLZ	VARCHAR2	10	None		

1 - 5 of 5

Table Operations [Help](#)

<input type="button" value="Job History"/>	The encryption operations that have been performed on this table.
<input type="button" value="Data Migration"/>	Data migration requires encryption settings specified for at least one column.
<input type="button" value="Delete Views and Triggers"/>	Remove views and triggers for this table on the database.
<input type="button" value="Key Rotation"/>	Re-encrypt selected columns in this table with new keys.
<input type="button" value="Unencrypt Columns"/>	The opposite of Data Migration. This removes the encryption settings from one or more columns in this table, and reverts those columns to their unencrypted state. You can re-encrypt the data later, so this is useful if upgrading your database.

Die Verschlüsselungs-Funktionalität ist nicht auf Datenbanken beschränkt. Durch Unterstützung von Standard APIs wie z.B. JCE, MSCAPI und XML ist die Erweiterung der Sicherheit auf der Ebene der Applikation gegeben; so kann auch jedes andere Datenhaltungssystem in das Sicherheitskonzept aufgenommen werden. Integriertes Load Balancing, Health Checking und Connection Pooling garantieren eine ausfallsichere und performante Integration in bestehende Systeme.

Mehr Information über DataSecure können Sie über info@clearnote.de oder +49 (0)40 7894 2287 anfordern.