

Im Folgenden werden stichpunktartig, und durch Grafiken verdeutlicht, die Vorteile einer Ingrian DataSecure Lösung für eine selektive Verschlüsselung und dadurch dem unberechtigten Zugriff entzogenen Daten in Oracle-Datenbanken dargestellt.

## Trennung von Schlüssel- und Datenbankadministration

- Klare Trennung von Oracle DBA Privilegien und DataSecure Admin-Rechten
- DataSecure Administrationsrechte unterschiedlich in diesen Blöcken definierbar:
  - Schlüsselmanagement
  - Konfiguration
  - Maintenance
  - Backup/Restore
- Detaillierte Rechtevergabe durch Unterkategorien

The screenshot displays the 'Administrator Configuration' window. On the left is a navigation tree with categories like System, Network, High Availability, Certificates, Administrators, SNMP, Logging, SSL, Certificate Authorities, Network-Attached Encryption, Server, Cluster, Keys, Authorization Policies, Local Users & Groups, LDAP Users & Groups, LDAP Server, Database Tools, Maintenance, Reports, and Help. The main area shows configuration for the 'Administrators' category.

**Administrator Configuration**

**Administrator Information**

Username:	gschildger
Full Name:	gerald schildger
Description:	
Password:	*****
Confirm Password:	*****
Password Expiration:	None

**Access Control - Device Configuration**

<input checked="" type="checkbox"/>	System and Network
<input checked="" type="checkbox"/>	High Availability
<input checked="" type="checkbox"/>	Certificates
<input checked="" type="checkbox"/>	Administrators
<input checked="" type="checkbox"/>	SNMP
<input checked="" type="checkbox"/>	Logging
<input checked="" type="checkbox"/>	SSL
<input checked="" type="checkbox"/>	Certificate Authorities

**Access Control - Network-Attached Encryption**

<input checked="" type="checkbox"/>	Cluster
<input checked="" type="checkbox"/>	NAE Server
<input checked="" type="checkbox"/>	NAE Keys and Authorization Policies
<input checked="" type="checkbox"/>	NAE Users, Groups, and LDAP
<input checked="" type="checkbox"/>	Database Tools

**Access Control - Maintenance**

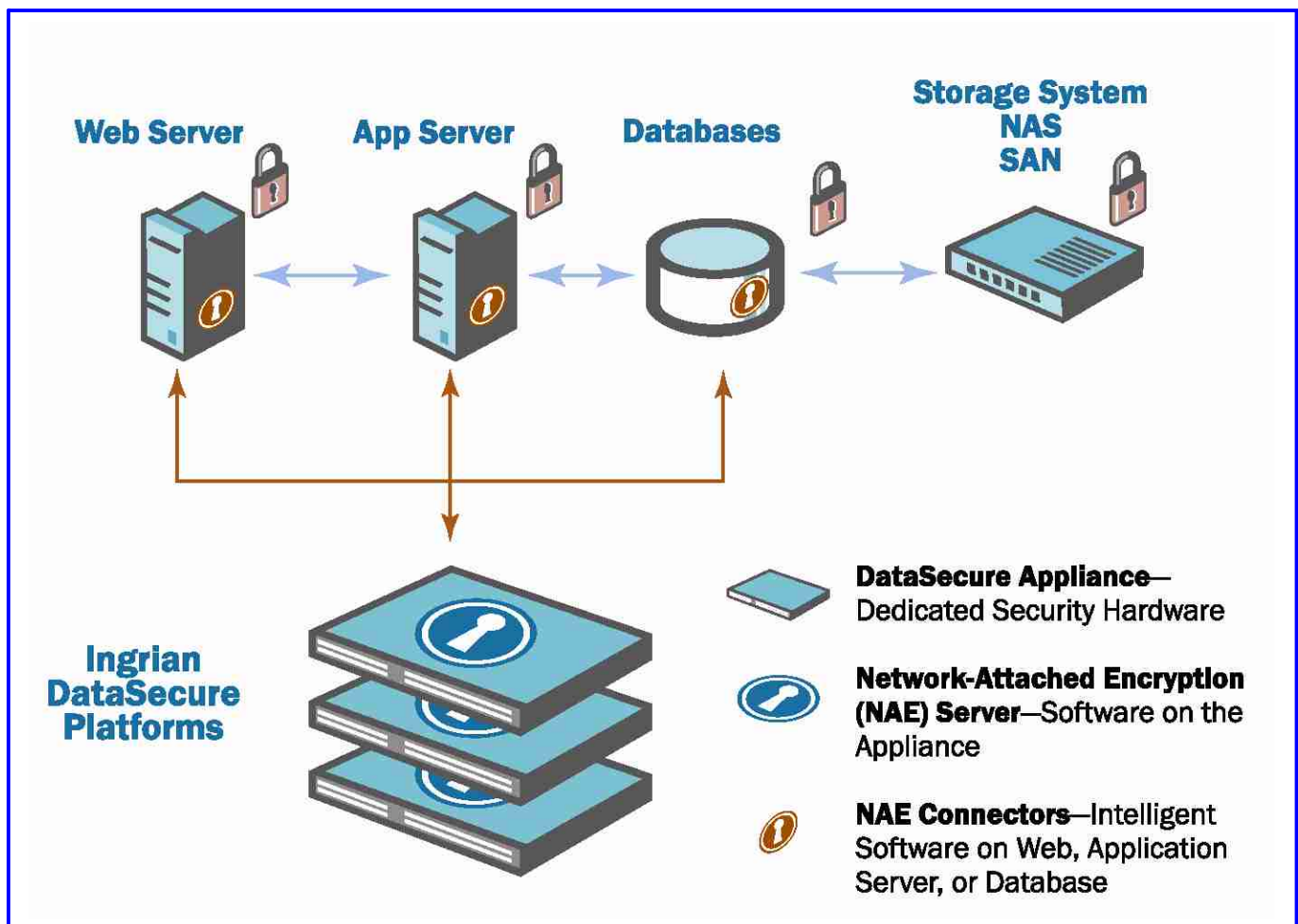
<input checked="" type="checkbox"/>	Services
<input checked="" type="checkbox"/>	Software Upgrade and System Health

**Access Control - Backup & Restore**

<input checked="" type="checkbox"/>	Backup Configuration
-------------------------------------	----------------------

## Flexible Integration

- unterstützt alle Oracle Releases, auch im Mix
- nahtlos einsetzbar auch in Verbindung mit anderen Plattformen
- Verschlüsselung auf Spaltenebene
- Integrierbar in verschiedenen Ebenen:
  - Datenbank  
über DB-Tools automatische Migration von zu verschlüsselnden Spalten
  - Application Server  
Einbindung in Java, .Net und XML
  - Web Server



## Zugriffskontrolle für Schlüssel

- Schlüsselzugriff autorisiert über Group/User
- auf Spaltenebene; nicht der Zugriff auf eine Tabelle wird bei fehlenden Rechten verhindert, sondern entsprechende Felder werden nur verschlüsselt angezeigt
- Schlüsselnutzung kann zeitlich eingeschränkt werden, so z.B. nur von 8.00 bis 18.00 Uhr
- Rechte zur Ver- oder Entschlüsselung können getrennt vergeben werden
- weitere Möglichkeiten der Einschränkung

**Network-Attached Encryption Key Configuration**

**NAE Key Properties**

Key Name:	ora-test-aes256
Owner Username:	Cleamote
Algorithm:	AES-256
Deletable:	<input type="checkbox"/>
Exportable:	<input type="checkbox"/>

Edit Back

**Group Permissions**

Items per page: 10 Submit

Group	Encrypt	Decrypt
NETusers	<input type="radio"/> Never <input checked="" type="radio"/> Always <input type="radio"/> Authorization Policy: authpol1	<input type="radio"/> Never <input checked="" type="radio"/> Always <input type="radio"/> Authorization Policy: authpol1

1 - 1 of 1

Save Cancel

## Autorisierungs-Policies

- vielfältige Kombinationen im Datenzugriff möglich:
  - User darf nur bestimmte Keys nutzen
  - Key darf nur zeitlich beschränkt verwendet werden
  - erlaubte Anzahl von Zugriffen auf Keys
  - Nur Encrypt oder Decrypt erlaubt
  - Exportable ja/nein
  - Deletable ja/nein

**Authorization Policy Configuration**

**Authorization Policy Properties** Help ?

Policy Name:

Maximum Operations per Hour:

**Authorized Usage Periods** Help ?

Items per page:

	Start Day	Start Time	End Day	End Time
<input checked="" type="checkbox"/>	Monday	00:00 (12:00 am)	Friday	19:00 (7:00 pm)
<input type="checkbox"/>	Saturday	07:00 (7:00 am)	Saturday	12:00 (12:00 pm)

1 - 2 of 2

## Logging und Auditing von Schlüsselzugriffen

- Logging von
  - Key Creation, Deletion, Property Änderung
  - jeder Encryption-Operation mit Nennung von Datum/Uhrzeit, Tabelle, Spalte, User, IP, Key
  - jeder Decryption-Operation wie oben
  - nicht autorisierten Zugriffen
  - Policy-konträren Zugriffen
- Log Download im Textformat möglich

**Database Encryption Logs**

Database Encryption Log Help

Log File: Current

Show Last Number of Lines: 25

Show Download Clear Rotate Now

```

Database Encryption Log:
2005-11-11 10:23:42 MigrateData Begin 192.168.0.6 medrec oratest: KUNDEN KONIGNR ingrian_example_key
2005-11-11 10:23:45 MigrateData Complete 192.168.0.6 medrec oratest: KUNDEN success 3
2005-11-11 14:37:40 MigrateData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:37:43 MigrateData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 0
2005-11-11 14:47:13 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:47:16 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 0
2005-11-11 14:48:33 MigrateData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:48:36 MigrateData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
2005-11-11 14:52:32 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:52:35 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
2005-11-11 14:55:05 MigrateData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:55:08 MigrateData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
2005-11-11 14:56:29 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 14:56:32 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
2005-11-11 15:05:30 MigrateData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2005-11-11 15:05:33 MigrateData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
2006-05-23 10:56:19 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2006-05-23 10:56:23 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE failure 0
2006-05-23 10:58:24 ResumeJob Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE --
2006-05-23 10:58:34 RestoreJob Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE --
2006-05-23 11:00:00 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2006-05-23 11:00:03 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE failure 0
2006-05-23 11:09:03 RestoreJob Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE --
2006-05-23 11:15:58 UnencryptData Begin 192.168.0.6 medrec oratest: TESTCOLREMOVE GEHALT ingrian_example_key
2006-05-23 11:16:01 UnencryptData Complete 192.168.0.6 medrec oratest: TESTCOLREMOVE success 3
    
```

## Daten Import / Export (ETL)

- ETL steht für Extract, Transform & Load
- Daten können beim Import schnell verschlüsselt werden
  - im Pre-Processing werden nur die sensitiven Spalten/Elemente verschlüsselt
  - Während des Loads keine Encryption, dadurch sehr schnell
- Beim Export keine zusätzlichen Sicherheitsmassnahmen nötig
  - Daten sind bereits verschlüsselt, werden als Ciphertext exportiert

## Schlüsselmanagement im PCI Kontext

- §3.4: Sensible Karten- und Inhaber-Daten müssen verschlüsselt werden, z.B. mit SHA-1, Triple-DES oder AES; gilt ebenfalls für alle Log-Dateien, Transport- und Sicherungsmedien
- §3.5 und §3.6: Schlüsselverwaltung
  - Eingeschränkter Zugriff auf Schlüssel
  - Schlüssel sollen nur an zugriffssicheren Orten gespeichert werden
  - Nutzung von "Strong Keys" (mindestens 128 bit)
  - Gesicherte Schlüsselverteilung und Speicherung
  - Periodischer Austausch der Schlüssel (Key rotation )
  - Zerstörung abgelaufener Schlüssel
  - Verhinderung unerlaubten Austauschs von Schlüsseln

Last but not least....

## Die DataSecure Familie

i311



i10



im Rack



i321



i110



Weitere Informationen auf [www.clearnote.de](http://www.clearnote.de),  
über [info@clearnote.de](mailto:info@clearnote.de) oder 040 78942287