

Oracle-Legitimation mit einer Standard-BI Lösung (SAS)
Christian Schütze
Metafinanz-Informationssysteme GmbH
München

Schlüsselworte

SAS 9.2, Oracle, Legitimation, BI, Rollen, VPD Virtual Private Database, FGAC, Fine Grained Access Control, RLS, Row Level Security

Einleitung

Daten in eine Oracle Datenbank zu laden ist der eine Schritt, aber ob und wie Fachanwender auf diese Daten zugreifen ein ganz anderer.

Aus der Praxis ergeben sich unterschiedliche Systemarchitekturen und fachliche, sowie technische Anforderungen an BI Lösungen. Nachfolgend wird an einem Praxisbeispiel die Umsetzung der Anforderungen an die Legitimationen und Datenzugriffe beschrieben. Im Vordergrund steht das Zusammenspiel einer Oracle Datenbank, zuständig für die Datenhaltung, und SAS 9.2, als Standard-BI Lösung für die Datenauswertung.

Die technischen Gegebenheiten sind ebenso zu berücksichtigen, wie fachliche Anforderungen an Dateneinschränkungen, Verschlüsselungen oder Zugriffsbeschränkungen.

Es gilt Oracle Rollen, Virtual Private Database und Standard-BI Suiten Hand in Hand zu nutzen um eine Lösung zu implementieren.

Legitimationen in Oracle Datenbanken

Der Titel des Themas deutet es bereits an – es geht um das Zusammenspiel von Oracle als Datenbank und SAS als BI Lösung. Um Interessierte aus beiden Welten ein gemeinsames Verständnis zu vermitteln zuerst ein kurzer Überblick über die Möglichkeiten Zugriffe auf Daten in einer Oracle Datenbank zu steuern.

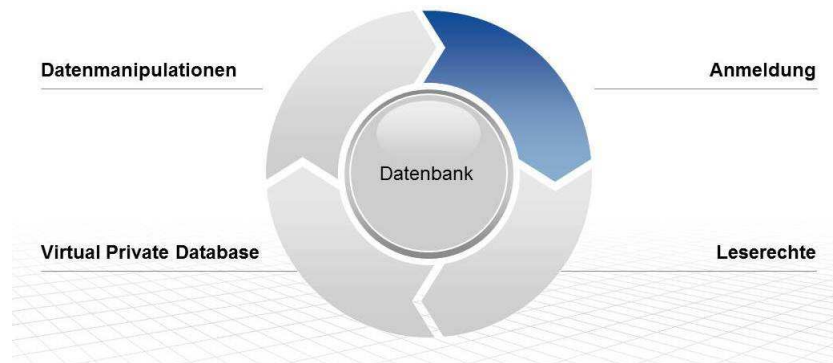


Abb. 1: vier aufeinander aufbauende Schritte die Datenzugriffe in Oracle Datenbanken zu steuern

Grundlegend ist im ersten Schritt das Vorhandensein eines Benutzernamens und Passworts, um eine Verbindung zur Datenbank herzustellen und sich anzumelden.

Standardmäßig hat man nach der Anmeldung nur Zugriff auf Daten im eigenen Schema. Der Zugriff auf Daten in anderen Schemata muss explizit erlaubt werden.

Dazu können mittels Grants auf einzelne Datenbankobjekte, wie Tabellen, Views oder Synonyme Leserechte vergeben werden. Um dies nicht pro Anwender durchführen zu müssen, bietet es sich an Rollen zu definieren, diesen Rollen den Zugriff auf Datenbankobjekte zu ermöglichen und einzelne Anwender einer oder mehreren Rollen zuzuordnen.

Nachdem man Leserechte auf eine Tabelle hat, gibt es in Oracle noch die Möglichkeit die enthaltenen Datensätze mittels Virtual Private Database(VPD) zu beschränken.

VPD ermöglicht es je nach Berechtigung eine Beschränkung der anzuzeigenden Datensätze zu definieren - ohne dass es dem Anwender transparent ist. Dies entspricht einem zusätzlichen Filter (Where-Bedingung), der bei jedem Zugriff auf die Tabelle angehängt und ausgeführt wird.

Eine weitere Oracle VPD Funktionalität bietet auch die Möglichkeit Inhalte einzelner Spalten einer Tabelle auszublenden.

Im Data Warehouse Umfeld reicht in der Regel eine Leseberechtigung aus, um Manipulationen der Dimensionen oder Fakten zu verhindern.

Für Datenmanipulationen bieten Oracle Datenbanken weitere Grants für Änderungsrechte (update, delete oder insert) oder Ausführungsrechte (execute) für PL/SQL Packages.

Überblick über die SAS 9.2 Welt

SAS ist die Abkürzung für Statistical Analysis System. Im folgenden Beispiel wird SAS 9.2 eingesetzt.

SAS 9.2 besitzt verschiedenen Komponenten, für die Definition von Berichten und Durchführen von Analysen ebenso wie zur Erstellung von Datenversorgungen (ETL).

Für das bessere Verständnis sollen einige Begriffe der SAS Welt eingeordnet und kurz erläutert werden. Der Fokus liegt auf den notwendigen Informationen, um das Zusammenspiel von SAS 9.2 und Oracle zu verstehen.

SAS bietet ein Webportal, über das Anwender vorhandene Berichte öffnen können. Eine weitere Webkomponente ist das Web Report Studio (WRS). Es erlaubt über den Browser einfache Berichte zu erstellen und zu speichern.

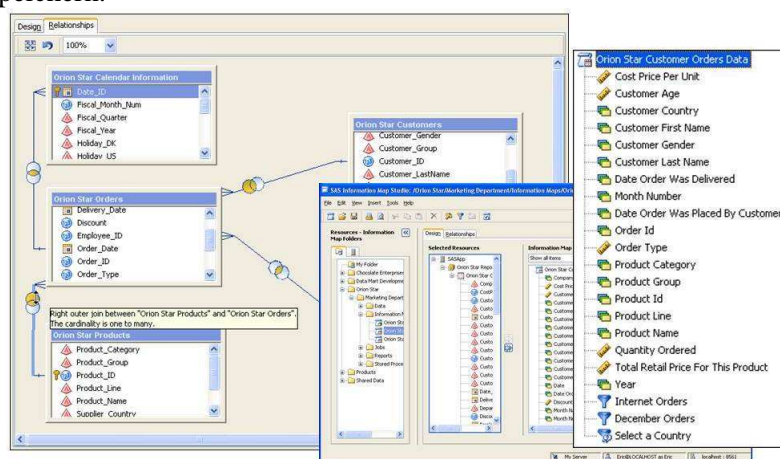


Abb. 2: Erstellung und Aufbau einer Information Map(Metadatenmodell)

Basis für die Verwendung des Web Report Studios sind Information Maps. Das sind Metadatenmodelle, die eine fachliche Sicht auf die physischen Daten z.B. in einer Oracle Datenbank darstellen. In den Metadatenmodellen sind die Joins zwischen Tabellen ebenso definiert, wie Filter und Aggregationsfunktionen von Kennzahlen. Bei der Verwendung muss der Anwender sich keine Gedanken machen, wie Tabellen zu verknüpfen oder wie die SQL Syntax ist.

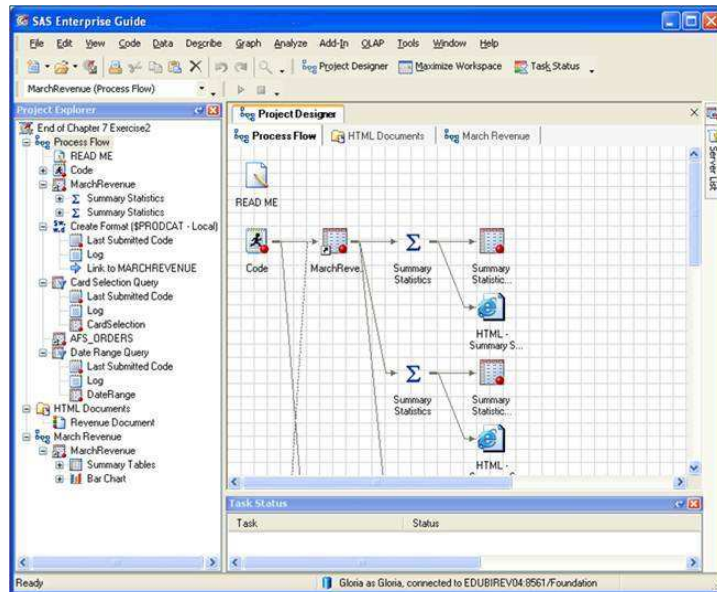


Abb. 3: Auswertung im Enterprise Guide

Die Windows-Anwendung SAS Enterprise Guide (EG) erlaubt es komplexere Berichte und Analyse zu erstellen. Man kann hierzu auf Information Maps oder direkt auf die Tabellen zugreifen. Die Ergebnisse der Abfragen können um neue Aggregationen oder Berechnungen erweitert werden. Schlussendlich kann das Ergebnis in verschiedenen grafischen Darstellungen (Listen, Kreuztabellen oder Grafiken) in unterschiedlichen Ausgabeformaten (PDF, XLS etc.) ausgegeben werden.

In SAS definiert man für die Verbindung zu Datenbanken sogenannte Libraries. Sie werden im Data Integration Studio angelegt. Das Data Integration Studio kann sonst für die Implementierung von ETL-Prozessen genutzt werden und bietet vergleichbare Funktionen wie der Oracle Warehouse Builder.

Information Maps, Berichte oder SAS Libraries werden in den SAS Metadaten gespeichert. Mittels SAS Gruppen und Rollen wird der Zugriff auf Berichte, Information Maps oder die technische Möglichkeit Berichte zu erstellen im Web Report Studio gesteuert. Für bestimmte Gruppen kann die Verwendung der einzelnen Komponenten beschränkt werden - bspw. die EG oder WRS Nutzung.

Architektur von Oracle Datenbank und SAS 9.2

In der Systemarchitektur des Beispiels dient eine Oracle Datenbank der Datenhaltung und als BI Suite für Auswertungen und Analysen wird SAS 9.2 eingesetzt.

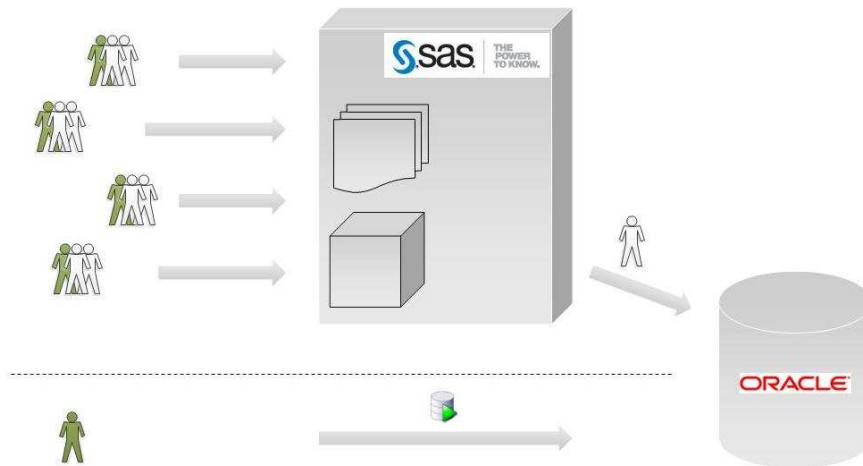


Abb. 4: Systemarchitektur

Die Anwender greifen über Information Maps im Web Report Studio oder mittels Enterprise Guide auf die Daten zu. Die ETL-Prozesse sind in PL/SQL implementiert.

Die notwendigen Daten für die Auswertungen (SAS Zugriff) befinden sich in einem separaten Datenbankschema.

Der Datenbankzugriff mittels SAS 9.2 erfolgt generell über einen technischen Oracle User für alle SAS Anwender. Man verzichtet darauf für jeden Anwender ein eigenes Login auf der Oracle Datenbank anzulegen und zu administrieren.

Eine kleine Anzahl von Anwendern, sogenannte „Poweruser“, hat zusätzlich einen persönlichen Login für die Oracle Datenbank und kann z.B. mittels SQL Plus darauf zugreifen.

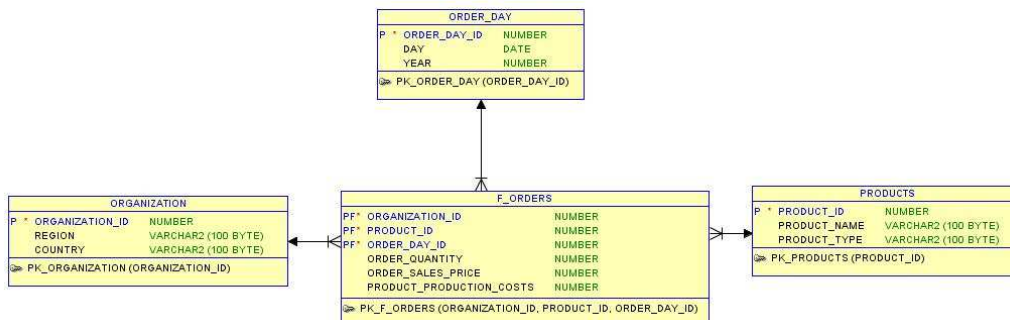


Abb. 5: Datenmodellierung in Form von Starschema

Die Datenablage erfolgt in Form von Starschemata mit Dimensionen- und Faktentabellen. Die konformen Dimensionen werden übergreifend in verschiedenen Datamarts wiederverwendet.

Realisierung der Anmeldung und Steuerung von Leserechten

Wie gerade erwähnt existieren „Poweruser“, die einen persönlichen Oracle Login erhalten. Sie können mittels SQL Plus oder SQL Developer eine Verbindung zur Datenbank aufbauen und eventuell weitere Tabellen benutzen, die ursprünglich nicht für die SAS Auswertungen vorgesehen sind.

Für die „Poweruser“ wurden Oracle Rollen definiert, die jeweils einen fachlichen Hintergrund haben. Diese Rollen erhalten wieder rum auf definierte Datenbankobjekte, meistens Tabellen, einen Grant um Daten zu selektieren. Die „Poweruser“ werden diesen Oracle Rollen zugeordnet.

Für den Zugriff aus SAS 9.2 auf die Oracle Datenbank wird ein technischer User angelegt. Dieser wird in der Definition der Datenbankverbindung (SAS Library) verwendet. Die Library wird außerdem so konfiguriert, dass es notwendig ist die einzelnen Datenbankobjekte, auf die zugegriffen werden soll, in

den SAS Metadaten registrieren zu müssen. Andernfalls sind die Oracle Tabellen in SAS unbekannt und können nicht verwendet werden.

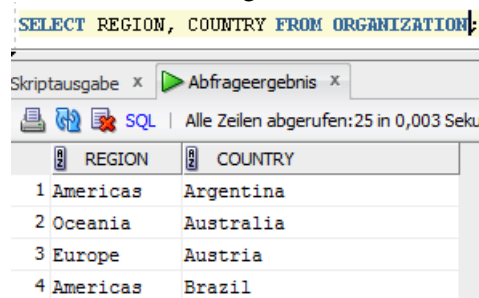
Das Standard- und Ad-hoc-Reporting wird in SAS 9.2 realisiert. Die meisten Anwender der BI Lösung benötigen demnach einen Zugriff auf die SAS Umgebung. Gleichzeitig erhalten die Anwender allerdings keinen persönlichen Zugriff auf die Daten in der Oracle Datenbank.

Um den Zugriff auf die Oracle Tabellen auch in SAS zu beschränken und zu steuern, werden dort ebenfalls themenspezifische SAS Rollen definiert. Die SAS Anwender werden diesen SAS Rollen zugeordnet.

Die Metadaten der registrierten Oracle Tabellen werden in SAS mittels der SAS Rollen abgesichert.

Realisierung fachlicher Anforderungen mittels VPD

Die Daten werden in Starschemata für die Auswertungen aufbereitet. Einige der zugehörigen Dimensionen enthalten Organisationsstrukturen, sogenannte Hierarchien.



```
SELECT REGION, COUNTRY FROM ORGANIZATION;
```

REGION	COUNTRY
1 Americas	Argentina
2 Oceania	Australia
3 Europe	Austria
4 Americas	Brazil

Abb. 6: Einteilung des Vertriebs in eine Hierarchie

Auf Basis dieser Hierarchien sollen Anwender ausschließlich bestimmte Informationen detailliert auswerten können. Andere Daten sollen ausgeblendet oder zusammengefasst dargestellt werden. Die Anwender werden wie bereits erwähnt in SAS bestimmten SAS Rollen zugeordnet. Aus der Kombination der zugeordneten Rollen ergibt sich für jeden Anwender eine individuelle Sicht der Daten (nur *Deutschland, Deutschland, Schweiz und Österreich* oder *Deutschland und Rest Europas*). Die Datenhaltung der Auswertungen und Dimensionen erfolgt wie eingangs beschrieben in einer Oracle Datenbank.

Die Umsetzung erfordert eine entsprechende Dimensionstabelle pro Anwender zu befüllen. Dazu ist es im ersten Schritt notwendig die Zuordnungen der Anwender zu SAS Rollen nach Oracle mittels SAS Stored Process zu transferieren.

USER	SAS_ROLLE
Müller	SAS Austria
Müller	SAS Germany
Müller	SAS Switzerland

Abb. 7: Informationen aus SAS zur Rolle je Anwender in Oracle

Im zweiten Schritt wird die ursprünglichen Dimension um eine Spalte „User“ erweitert und mittels PL/SQL auf Basis der vergebenen SAS Rollen befüllt. Im Endergebnis existiert eine Dimension mit individuellen Einträgen je Anwender.

```
select REGION, COUNTRY, "USER" from sas_organization;
```

	REGION	COUNTRY	USER
1	Europe	Austria	Müller
2	Europe	Switzerland	Müller
3	Europe	Germany	Müller
4	Europe	Austria	Schmidt
5	Europe	Switzerland	Schmidt
6	Europe	Germany	Schmidt
7	Europe	Others	Schmidt

Abb. 8: Hierarchie je Anwender

Für die korrekte Selektion der Einträge aus der erweiterten Dimension werden eine Policy Funktion in einer Policy verwendet.

```
begin
DBMS_RLS.ADD_POLICY(
  object_schema      => 'SASUSER',
  object_name        => 'SAS_ORGANIZATION',
  policy_name        => 'POL_ORGANIZATION',
  function_schema    => 'SASUSER',
  policy_function     => 'F_AUTH_ORGANIZATION',
  statement_types    => 'SELECT',
  update_check       => false,
  enable             => true,
  static_policy      => false
);
end;
```

Abb. 9: Definition der Policy

```
CREATE OR REPLACE FUNCTION "SASUSER"."F_AUTH_ORGANIZATION" (
object_schema IN VARCHAR2,
object_name VARCHAR2)
RETURN VARCHAR2
IS
  v_user varchar2(100);
BEGIN
  v_user := case when PKG_AUTH_SAS_SESSION.get_user is null then upper(user) else PKG_AUTH_SAS_SESSION.get_user end;
  if v_user in ( 'SASUSER' ) then
    return '1=1';
  else
    return 'user = ''' || v_user || '''';
  end if;
END;
```

Abb. 9: Definition der Policy Funktion

Um Oracle den in SAS angemeldeten Anwender mitzuteilen, muss diese Information noch von SAS nach Oracle übertragen werden. Zu Lösung wird in der SAS Library eine PL/SQL Prozedur aufgerufen, deren Parameter Session-Variablen aus SAS sind.

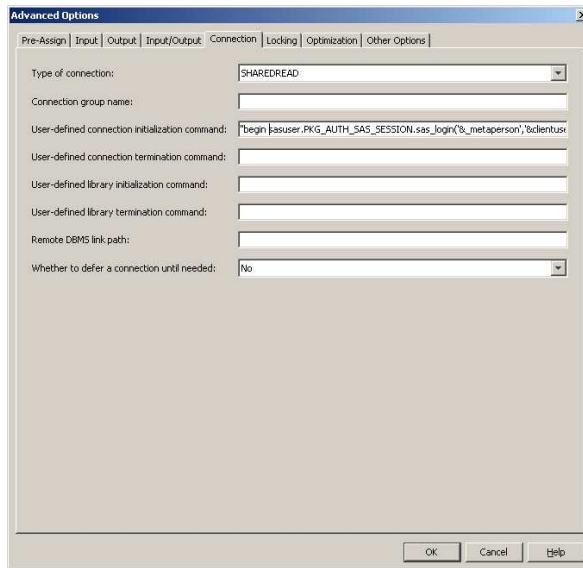


Abb. 10: Aufruf der PL/SQL Prozedur in SAS Library zu finden unter Properties > Options > Advanced Options

Die benutzten Variablen enthalten je nach SAS Komponente den angemeldeten Benutzer.

```
begin
sasuser.PKG_AUTH_SAS_SESSION.sas_login('&metaperson', '&clientuserid', '&sysuserid', '&syshostname');
end;
```

Abb. 11: Aufruf für PL/SQL Prozedur mit Übergabe der Session-Variablen aus SAS

Das Package PKG_AUTH_SAS_SESSION speichert die Parameter in einer PL/SQL Variablen, welche durch die Policy Funktion genutzt werden kann. Damit ist die Kommunikation zwischen SAS und Oracle gewährleistet.

Zusätzlich sollen die Daten einiger Faktentabellen übergreifend von Verantwortlichen verschiedener Themengebiete genutzt werden. Diese sollen aber nur eine bestimmte Auswahl von Kennzahlen zur Auswertung verwenden können.

Damit man in SAS weiterhin die gleichen Information Maps verwenden kann, werden diese Kennzahlen/Tabellenspalten immer mit NULL ausgewiesen.

```
select REGION, COUNTRY, ORDER_DAY_ID as DAY,
ORDER_QUANTITY,
ORDER_SALES_PRICE, PRODUCT_PRODUCTION_COSTS
, PRODUCT_NAME, PRODUCT_TYPE from ORGANIZATION ,F_ORDERS , PRODUCTS where order_day_id = to_date('02042001', 'ddmmyyyy')
and product_name = 'Fly Fishing' ;
```

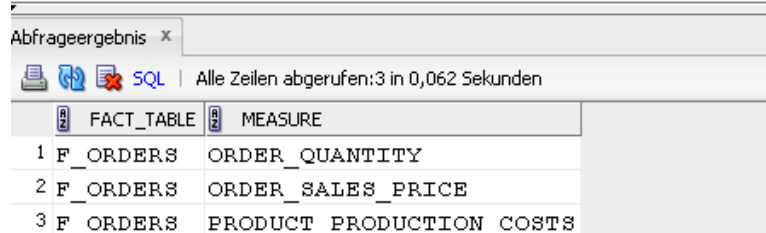
REGION	COUNTRY	DAY	ORDER_QUANTITY	ORDER_SALES_PRICE	PRODUCT_PRODUCTION_COSTS	PRODUCT_NAME	PRODUCT_T
1 Europe	Germany	02.04.01	132	1215,99	1101,99	Fly Fishing	Electronics
2 Europe	Germany	02.04.01	48	15,99	10,99	Fly Fishing	Electronics

REGION	COUNTRY	DAY	ORDER_QUANTITY	ORDER_SALES_PRICE	PRODUCT_PRODUCTION_COSTS	PRODU
1 Europe	Germany	02.04.01	132	1215,99	0	Fly Fish.
2 Europe	Germany	02.04.01	48	15,99	0	Fly Fish.
3 Europe	Germany	02.04.01	3	40,99	0	Fly Fish.

Abb. 12: Eine SQL-Abfrage liefert je Berechtigung einmal Werte für die Kennzahlen und bei eingeschränkter Berechtigung sind die Werte durch NULL ersetzt.

Bei der Umsetzung kommt wieder VPD zum Einsatz. Die zugehörige Funktion nutzt generisch eine von den Fachanwendern definierte Negativliste der ausgeblendeten Kennzahlen je Oracle Tabelle.

```
select FACT_TABLE, MEASURE from SAS_LEGI_COLUMNS
```



The screenshot shows a SQL query result in a window titled 'Abfrageergebnis'. The query is 'select FACT_TABLE, MEASURE from SAS_LEGI_COLUMNS'. The result is a table with two columns: 'FACT_TABLE' and 'MEASURE'. There are three rows of data.

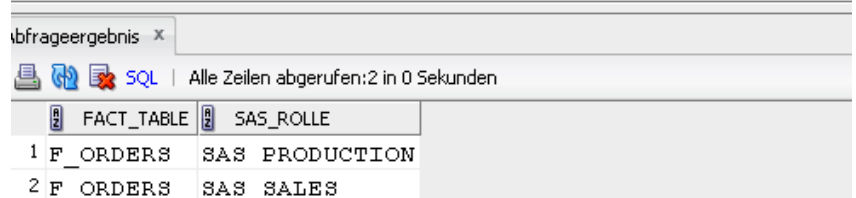
	FACT_TABLE	MEASURE
1	F_ORDERS	ORDER_QUANTITY
2	F_ORDERS	ORDER_SALES_PRICE
3	F_ORDERS	PRODUCT_PRODUCTION_COSTS

Abb. 13: Kennzahlen je Faktentabelle

Die zugehörige Policy verwendet die optionalen Parameter `sec_relevant_cols` und `sec_relevant_cols_opt`.

Die SAS Rollen, die Zugriff auf die ausgeblendeten Kennzahlen bekommen sollen, werden in einer weiteren Tabelle definiert.

```
select FACT_TABLE, SAS_ROLLE from SAS_LEGI_COLUMNS_ROLE;
```



The screenshot shows a SQL query result in a window titled 'Abfrageergebnis'. The query is 'select FACT_TABLE, SAS_ROLLE from SAS_LEGI_COLUMNS_ROLE;'. The result is a table with two columns: 'FACT_TABLE' and 'SAS_ROLLE'. There are two rows of data.

	FACT_TABLE	SAS_ROLLE
1	F_ORDERS	SAS PRODUCTION
2	F_ORDERS	SAS SALES

Abb. 14: Festlegung SAS-Rollen mit vollem Zugriff

Die Anwender haben die Möglichkeit zusätzlich Datenänderungen für Beschriftungen von Dimensionen vorzunehmen. Seitens IT ist es allerdings nicht erwünscht, dass die Änderungen direkt in den Dimensionstabellen vorgenommen werden sollen.

Die Fachbereiche erhalten Änderungsrechte auf Views. Mittels Triggern werden die Daten in separaten Tabellen gespeichert. Diese dient zur Befüllung der Dimensionen und die enthaltenen Datensätze werden in den folgenden Ladeprozessen berücksichtigt.

Weiterhin wird in SAS selbst der Zugriff auf die vorhandenen Information Maps und Berichte mittels SAS Rollen gesteuert.

Fazit

Bei der Konzeption und Implementierung der Legitimationsanforderungen hat sich gezeigt, dass es essentiell ist ein tiefgreifendes Wissen zu den Funktionen und Möglichkeiten in Oracle und SAS zu haben.

Dies ist die Basis, um die Probleme und Herausforderungen beim Zusammenspiel von Oracle Datenbank und SAS zu meistern. Versuche die Anforderungen alleine in SAS oder Oracle abzudecken führen zu komplexen Umsetzungen und sind durch vorhandene Vorgaben auch nicht möglich.

Für die Umsetzung ist ein Prototyp unerlässlich. Mit ihm können und sollten alle fachlichen Anforderungen und ihre Lösungsmöglichkeiten validiert werden. Mit der Implementierung können und werden Prozesse innerhalb der IT und zwischen Fachanwender und IT definiert. Diese erleichtern im weiteren Verlauf die Implementierungen und dienen als Leitfaden durch das komplexe Zusammenspiel von Datenbank und BI Lösung.

Kontaktadresse:

Christian Schütze
Metafinanz-Informationssysteme GmbH
Leopoldstraß 46
D-80804 München

Telefon: +49 (0) 89-36053150
Fax: +49 (0) 89-36053115
E-Mail: Christian.Schuetze@metafinanz.de
Internet: <http://www.metafinanz.de>