Bayer CropScience

BioScience

Multiple crop in a single database using Oracle

Summary Slide

- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

Summary Slide

- Goals
- Security solutions
  - Application security
  - View security
  - Virtual Private Database (VPD)
- What is VPD?
- Security requirements
  - Security implementation
- ICIS constraints
  - Issues with the INSTLN and USERS table
- Conclusions

Goals

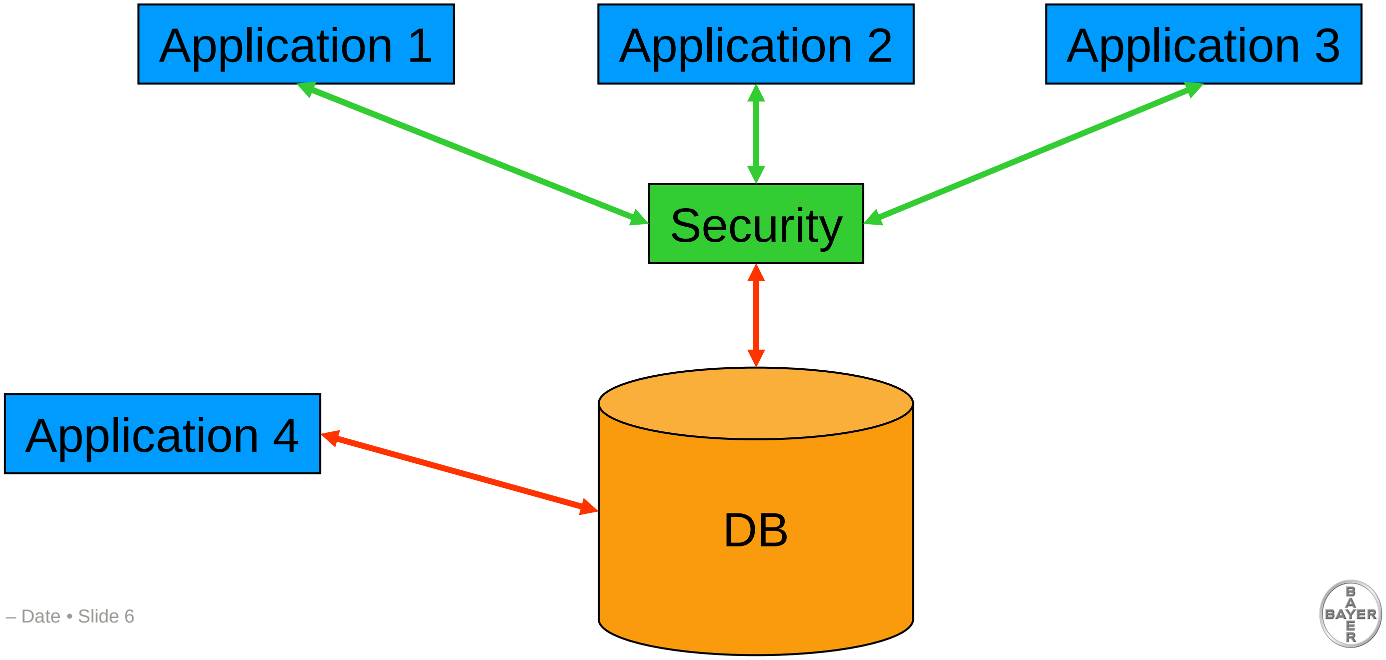
- **Gather all ICIS databases into a unique repository**
  - Make the maintenance easier
  - Avoid data transfer
  - Faster deployment
- **Apply security rules based on groups of users and crops**
- **Keep the ICIS developments as generic as possible**
  - The security rules do not have to impact the ICIS tools

Summary Slide

- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

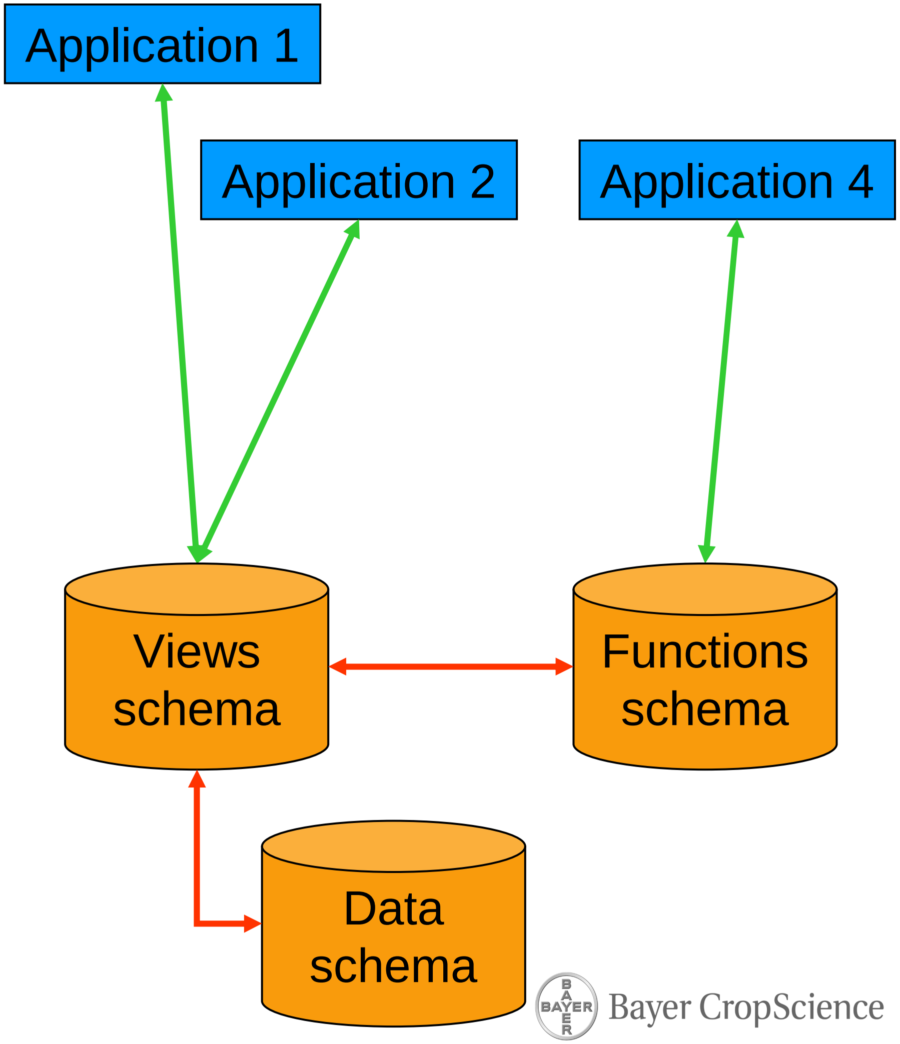
Security solutions (1)

- **Apply the security at the application level**
  - The security rules have to be implemented in each application.
    - Security inconsistencies may appear.
- **Database is not secured.**



Security solutions (2)

- **Use a view on the top of the table**
  - You must then restrict access to the table.
  - What happen if a user needs to access to the table.
    - You must then create additional views and roles
  - What happen if you build a function making updates on the table.
    - The function should only access to the views.
- **Multiplication of roles and privileges**



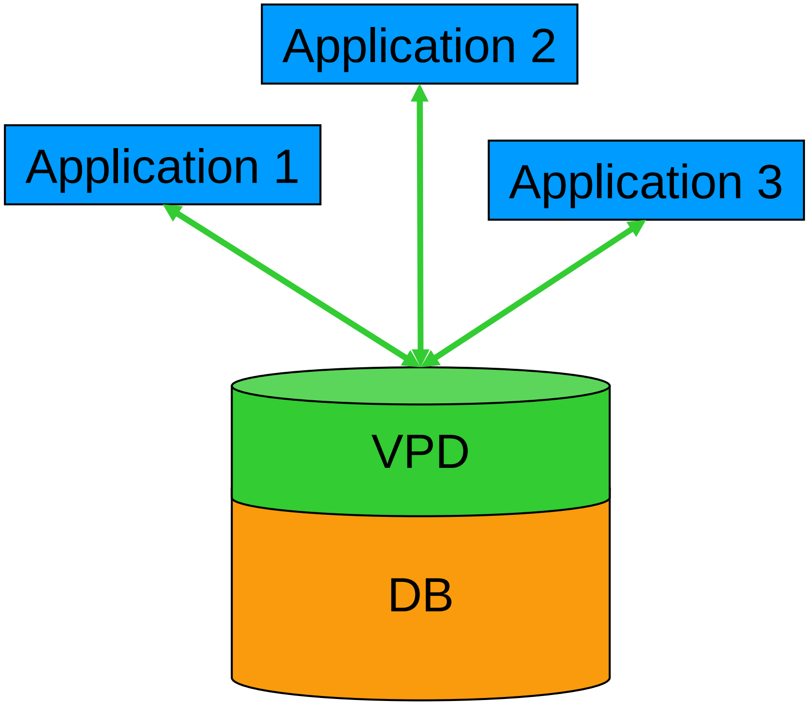
Bayer CropScience

Security solutions (3)

- The security is applied at the table level

- Virtual Private Database
  - Row-Level Security
  - Fine-Grained Access Control

- *“VPD allows you to define security policies on tables (and specific types of operations on tables) that have the effect of restricting which rows a user can see or change in a table.”*



Summary Slide

- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

What is VPD?

- ***VPD consists of three main components***
  - *Policy*
    - ➢ *A declarative command that determines when and how to apply security.*
  - *Policy function*
    - ➢ *A PL/SQL function that is called whenever the condition specified in the policy are met.*
  - *Predicate*
    - ➢ *A string that is generated by the policy function, and then applied to the users' SQL statements, indicating limiting condition.*
- ***Implemented with the package DBMS_RLS***
- ***Fully integrated to the Oracle engine***

What is VPD? - example

Predicate

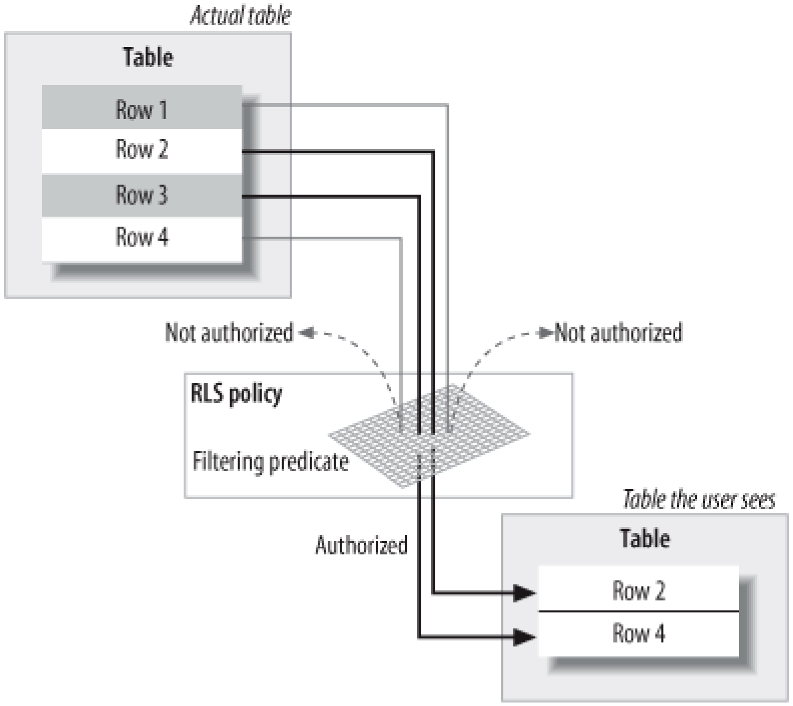
- A user can only see his germplasm list
  - listuid in (
    SELECT userid
    FROM users
    WHERE uname=USER)

ICIS SetGen run query

- SELECT listid, listname, listdesc
  FROM listnms;

VPD modifies the query by adding the predicate

- SELECT listid, listname, listdesc
  FROM listnms
  WHERE listuid in (
  SELECT userid
  FROM users
  WHERE uname=USER);



Summary Slide

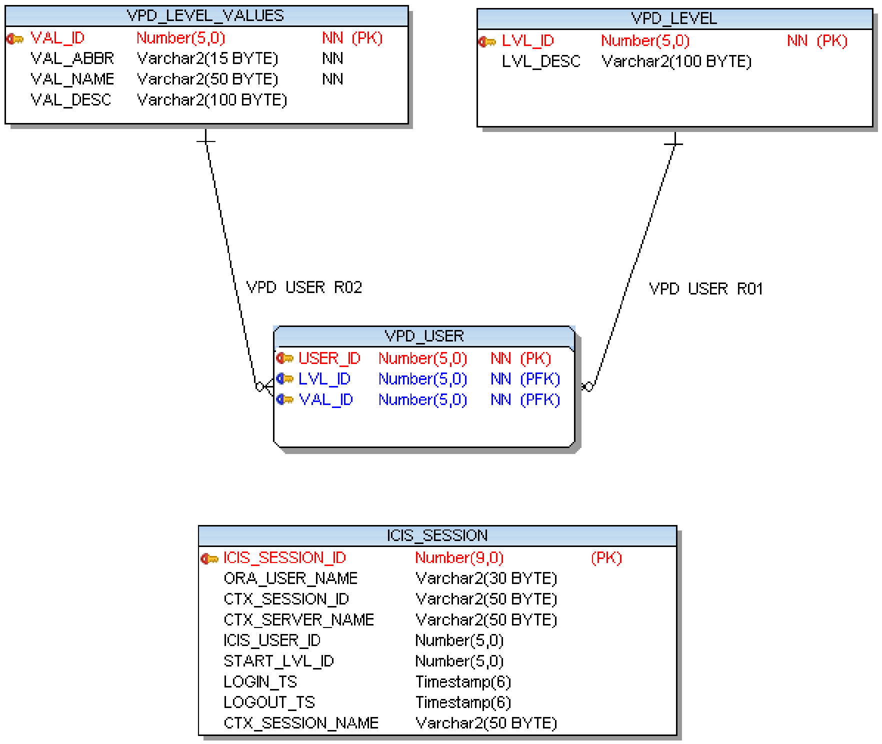
- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

Security requirements

- **Security requirements**
  - A user is described by description levels
    - Family, Crop, Location, Team, Function, Person, Access right…
  - Each level allows access to a set of data
  - Data are private to a user
  - Data can be shared within user groups or public to a crop
- **Implementation**
  - Security tables
  - Security fields
  - Security functions
  - Security policies

Security tables (1)

- **VPD_LEVEL**
  - Store the level descriptors
    - Crop, Location, Person…
- **VPD_LEVEL_VALUES**
  - Store the level values
    - Rice, CU
    - IND, NUN
    - CSFDS, NLCBOO
- **VPD_USER**
  - Associate a value to a level
- **ICIS_SESSION**
  - Manage ICIS session information when connecting to the database



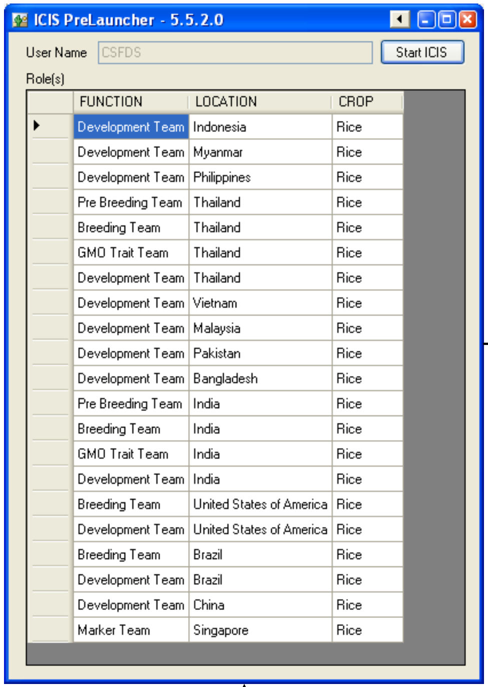
VPD_LEVEL_VALUES		
VAL_ID	Number(5,0)	NN (PK)
VAL_ABBR	Varchar2(15 BYTE)	NN
VAL_NAME	Varchar2(50 BYTE)	NN
VAL_DESC	Varchar2(100 BYTE)	

VPD_LEVEL		
LVL_ID	Number(5,0)	NN (PK)
LVL_DESC	Varchar2(100 BYTE)	

VPD_USER		
USER_ID	Number(5,0)	NN (PK)
LVL_ID	Number(5,0)	NN (PFK)
VAL_ID	Number(5,0)	NN (PFK)

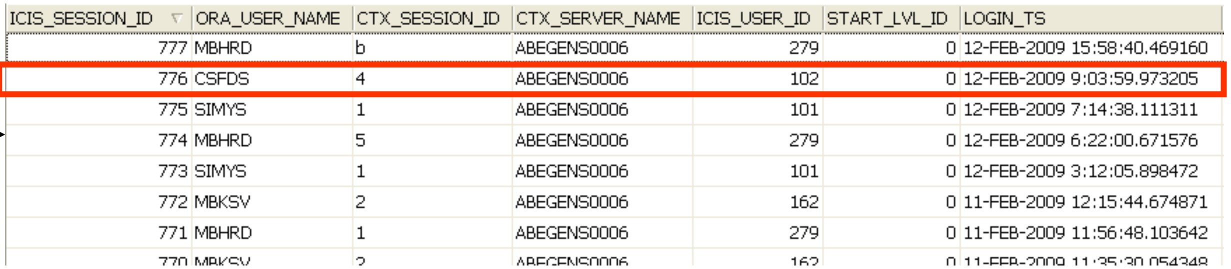
ICIS_SESSION		
ICIS_SESSION_ID	Number(9,0)	(PK)
ORA_USER_NAME	Varchar2(30 BYTE)	
CTX_SESSION_ID	Varchar2(50 BYTE)	
CTX_SERVER_NAME	Varchar2(50 BYTE)	
ICIS_USER_ID	Number(5,0)	
START_LVL_ID	Number(5,0)	
LOGIN_TS	Timestamp(6)	
LOGOUT_TS	Timestamp(6)	
CTX_SESSION_NAME	Varchar2(50 BYTE)	

Security tables (2)



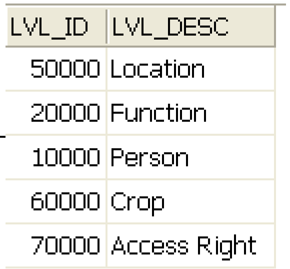
FUNCTION	LOCATION	CROP
Development Team	Indonesia	Rice
Development Team	Myanmar	Rice
Development Team	Philippines	Rice
Pre Breeding Team	Thailand	Rice
Breeding Team	Thailand	Rice
GMO Trait Team	Thailand	Rice
Development Team	Thailand	Rice
Development Team	Vietnam	Rice
Development Team	Malaysia	Rice
Development Team	Pakistan	Rice
Development Team	Bangladesh	Rice
Pre Breeding Team	India	Rice
Breeding Team	India	Rice
GMO Trait Team	India	Rice
Development Team	India	Rice
Breeding Team	United States of America	Rice
Development Team	United States of America	Rice
Breeding Team	Brazil	Rice
Development Team	Brazil	Rice
Development Team	China	Rice
Marker Team	Singapore	Rice

ICIS_SESSION



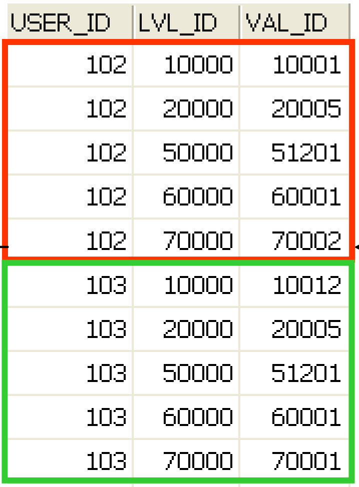
ICIS_SESSION_ID	ORA_USER_NAME	CTX_SESSION_ID	CTX_SERVER_NAME	ICIS_USER_ID	START_LVL_ID	LOGIN_TS
777	MBHRD	b	ABEGENS0006	279	0	12-FEB-2009 15:58:40.469160
776	CSFDS	4	ABEGENS0006	102	0	12-FEB-2009 9:03:59.973205
775	SIMYS	1	ABEGENS0006	101	0	12-FEB-2009 7:14:38.111311
774	MBHRD	5	ABEGENS0006	279	0	12-FEB-2009 6:22:00.671576
773	SIMYS	1	ABEGENS0006	101	0	12-FEB-2009 3:12:05.898472
772	MBKSV	2	ABEGENS0006	162	0	11-FEB-2009 12:15:44.674871
771	MBHRD	1	ABEGENS0006	279	0	11-FEB-2009 11:56:48.103642
770	MBKSV	2	ABEGENS0006	162	0	11-FEB-2009 11:35:30.054348

VPD_LEVEL



LVL_ID	LVL_DESC
50000	Location
20000	Function
10000	Person
60000	Crop
70000	Access Right

VPD_USER

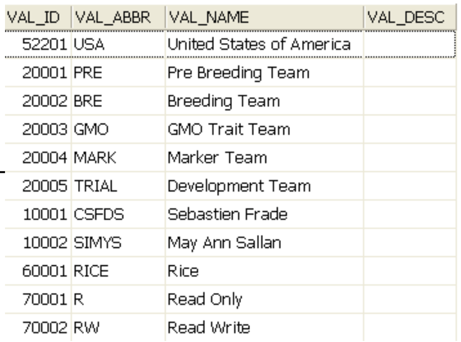


USER_ID	LVL_ID	VAL_ID
102	10000	10001
102	20000	20005
102	50000	51201
102	60000	60001
102	70000	70002
103	10000	10012
103	20000	20005
103	50000	51201
103	60000	60001
103	70000	70001

Role

Role

VPD_LEVEL_VALUES



VAL_ID	VAL_ABBR	VAL_NAME	VAL_DESC
52201	USA	United States of America	
20001	PRE	Pre Breeding Team	
20002	BRE	Breeding Team	
20003	GMO	GMO Trait Team	
20004	MARK	Marker Team	
20005	TRIAL	Development Team	
10001	CSFDS	Sebastien Frade	
10002	SIMYS	May Ann Sallan	
60001	RICE	Rice	
70001	R	Read Only	
70002	RW	Read Write	

Security fields

- **Extra fields have been added to ALL ICIS tables**
  - INSID
    - The ICIS user ID who inserted a record
  - INSDATE
    - Timestamp adding record
  - UPDID
    - The user ID who updated a record
  - UPDDATE
    - Timestamp updating record
  - VPD_PUBLIC
    - Define a shared entry
- **Automatically filled by Oracle triggers**
- **INSID used by VPD to restrict access rights**

Security functions

- As the same fields are available in all tables, generic functions can be used to restrict the rows a user can see
- A function can be called by multiple policies
- Return a specific predicate based on the access rights of the chosen role

Security policies

- A declarative command that determines when and how to apply the policy
- It is specific to a schema object
  - Table, view or synonym
- It calls a VPD function
- Can control one or more statement types
  - Select, Insert, Update, Delete or Index
- Can enforce security on column

```
BEGIN
 DBMS_RLS.ADD_POLICY    (
   object_schema         => 'ICISL'
   ,object_name          => 'LISTNMS'
   ,policy_name          => 'POL_LISTNMS'
   ,function_schema       => 'ICISSEC'
   ,policy_function       => 'PKG_ICIS_VPD.VPD_LOC_FUNC_CROP'
   ,statement_types       => 'SELECT,INSERT,UPDATE,DELETE,INDEX'
   ,policy_type          => dbms_rls.dynamic
   ,long_predicate        => FALSE
   ,sec_relevant_cols      => 'LISTNAME,LISTDATE,LISTTYPE,LISTUID,
                              LISTDESC,LISTSTATUS, LHIERARCHY,
                              INSID,INSDATE,UPDID,UPDDATE,VPD_PUBLIC'
   ,sec_relevant_cols_opt => NULL
   ,update_check         => FALSE
   ,static_policy        => FALSE
   ,enable              => TRUE );
END;
/
```

ICIS VPD by example

- **LISTNMS table ➔Filtered on Crop level**
  - 1000 records, 4 crops (250 rows/crop), GID-range -1 to -1000
- **Application-SQL, connected as member of one of any crop**
  - SELECT * FROM icisl.listnms;
    - Result: 250 rows
  - SELECT count(listname) FROM icisl.listnms;
    - Result: 250 rows
  - SELECT count(listid) FROM icisl.listnms;
    - Result: 1000 rows (VPD not applied on primary key LISTID)
  - SELECT min(listid) FROM icisl.listnms;
    - Result: -1000 (Mandatory to add a new record)

Summary Slide

- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

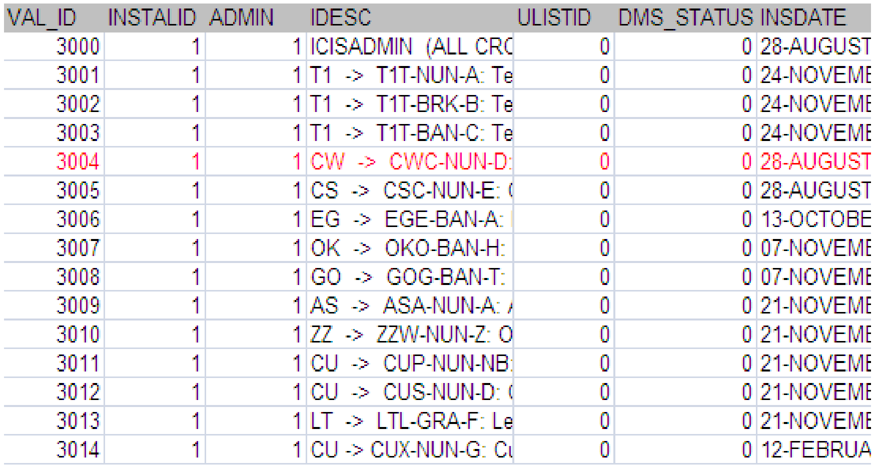
ICIS constraints

- **The INSTLN table contains the database descriptions**
  - The databases are distinguished by different Ids
  - Only one row in ICISL.INSTLN must be present.
- **The USERS table contains the user descriptions**
  - The USERS table does not allow duplicates user name
  - A person may have several ICIS user ID, so several user name
  - One Oracle login per ICIS user ID
    - Lot of Oracle user maintenance

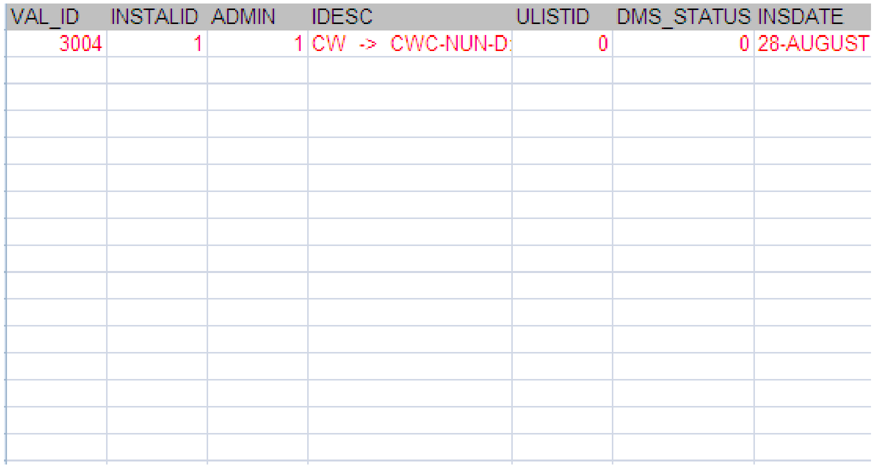
INSTLN table

- **Constraint**
  - Only one row in ICISL.INSTLN must be present
- **Goal**
  - During a session, the ICISL.INSTLN table must return only one row.
- **Solution**
  - Filter the entries based on the access right of the person
- **Defined a policy for the table INSTLN in the ICISL schema**
- **Defined a specific function**
  - The predicate will return only one row

Before filter



VAL_ID	INSTALID	ADMIN	IDESC	ULISTID	DMS_STATUS	INSDATE
3000	1	1	ICISADMIN (ALL CR	0	0	28-AUGUST
3001	1	1	T1 -> T1T-NUN-A: Te	0	0	24-NOVEM
3002	1	1	T1 -> T1T-BRK-B: Te	0	0	24-NOVEM
3003	1	1	T1 -> T1T-BAN-C: Te	0	0	24-NOVEM
3004	1	1	CW -> CWC-NUN-D:	0	0	28-AUGUST
3005	1	1	CS -> CSC-NUN-E:	0	0	28-AUGUST
3006	1	1	EG -> EGE-BAN-A:	0	0	13-OCTOBE
3007	1	1	OK -> OKO-BAN-H:	0	0	07-NOVEM
3008	1	1	GO -> GOG-BAN-T:	0	0	07-NOVEM
3009	1	1	AS -> ASA-NUN-A:	0	0	21-NOVEM
3010	1	1	ZZ -> ZZW-NUN-Z: O	0	0	21-NOVEM
3011	1	1	CU -> CUP-NUN-NB:	0	0	21-NOVEM
3012	1	1	CU -> CUS-NUN-D:	0	0	21-NOVEM
3013	1	1	LT -> LTL-GRA-F: Le	0	0	21-NOVEM
3014	1	1	CU -> CUX-NUN-G: C	0	0	12-FEBRUA



VAL_ID	INSTALID	ADMIN	IDESC	ULISTID	DMS_STATUS	INSDATE
3004	1	1	CW -> CWC-NUN-D:	0	0	28-AUGUST

Bayer CropScience

USERS table

Constraint

- The USERS table does not allow duplicates user name

Goal

- During a session, the current user name must appear only once
- Minimize as much as possible the Oracle user maintenance
  - One person connected to ICIS = One Oracle user

Solution

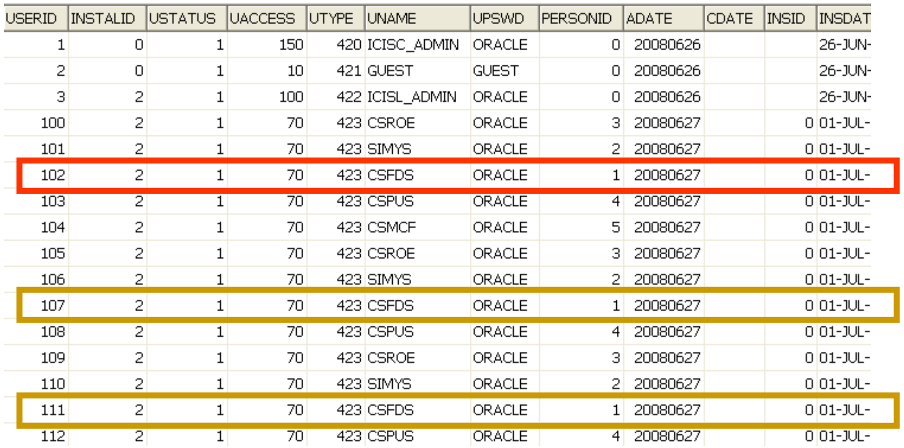
- Apply VPD filtering on the USERS table
  - For the current connected person, only retrieve one ICIS user ID

Defined a policy for the table USERS in the ICISC schema

Defined a specific function

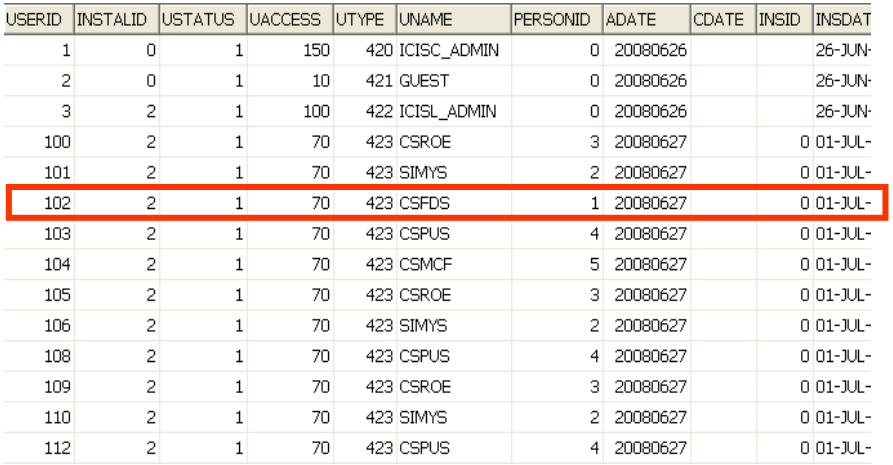
- The predicate will return
  - The row of the chosen ICIS user ID of the connected person
  - All the other person's ICIS user id

Before filter



USERID	INSTALID	USTATUS	UACCESS	UTYPE	UNAME	UPSWD	PERSONID	ADATE	CDATE	INSID	INSDAT
1	0	1	150	420	ICISC_ADMIN	ORACLE	0	20080626			26-JUN-
2	0	1	10	421	GUEST	GUEST	0	20080626			26-JUN-
3	2	1	100	422	ICISL_ADMIN	ORACLE	0	20080626			26-JUN-
100	2	1	70	423	CSROE	ORACLE	3	20080627		0	01-JUL-
101	2	1	70	423	SIMYS	ORACLE	2	20080627		0	01-JUL-
102	2	1	70	423	CSFDS	ORACLE	1	20080627		0	01-JUL-
103	2	1	70	423	CSPUS	ORACLE	4	20080627		0	01-JUL-
104	2	1	70	423	CSMCF	ORACLE	5	20080627		0	01-JUL-
105	2	1	70	423	CSROE	ORACLE	3	20080627		0	01-JUL-
106	2	1	70	423	SIMYS	ORACLE	2	20080627		0	01-JUL-
107	2	1	70	423	CSFDS	ORACLE	1	20080627		0	01-JUL-
108	2	1	70	423	CSPUS	ORACLE	4	20080627		0	01-JUL-
109	2	1	70	423	CSROE	ORACLE	3	20080627		0	01-JUL-
110	2	1	70	423	SIMYS	ORACLE	2	20080627		0	01-JUL-
111	2	1	70	423	CSFDS	ORACLE	1	20080627		0	01-JUL-
112	2	1	70	423	CSPUS	ORACLE	4	20080627		0	01-JUL-

After filter



USERID	INSTALID	USTATUS	UACCESS	UTYPE	UNAME	PERSONID	ADATE	CDATE	INSID	INSDAT
1	0	1	150	420	ICISC_ADMIN	0	20080626			26-JUN-
2	0	1	10	421	GUEST	0	20080626			26-JUN-
3	2	1	100	422	ICISL_ADMIN	0	20080626			26-JUN-
100	2	1	70	423	CSROE	3	20080627		0	01-JUL-
101	2	1	70	423	SIMYS	2	20080627		0	01-JUL-
102	2	1	70	423	CSFDS	1	20080627		0	01-JUL-
103	2	1	70	423	CSPUS	4	20080627		0	01-JUL-
104	2	1	70	423	CSMCF	5	20080627		0	01-JUL-
105	2	1	70	423	CSROE	3	20080627		0	01-JUL-
106	2	1	70	423	SIMYS	2	20080627		0	01-JUL-
108	2	1	70	423	CSPUS	4	20080627		0	01-JUL-
109	2	1	70	423	CSROE	3	20080627		0	01-JUL-
110	2	1	70	423	SIMYS	2	20080627		0	01-JUL-
112	2	1	70	423	CSPUS	4	20080627		0	01-JUL-

Summary Slide

- **Goals**
- **Security solutions**
  - Application security
  - View security
  - Virtual Private Database (VPD)
- **What is VPD?**
- **Security requirements**
  - Security implementation
- **ICIS constraints**
  - Issues with the INSTLN and USERS table
- **Conclusions**

Conclusions

- **Gather all ICIS databases into a unique repository**
  - Limit the number of schemas to 4 (ICISC, ICISL, ICISV and ICISSEC)
  - Crop data dynamically filtered by VPD, no more data transfer
  - All teams and crops data in the unique local database
- **Apply security rules based on groups of users and crops**
  - Extended the ICIS data model to support the level descriptors (ICISSEC)
  - VPD filters data according to a specific person role
- **Keep the ICIS developments as generic as possible**
  - Only the DLL has been modified to support the registration process
  - Added the SESSION_ID key in the [DLL SETTINGS] section of the INI file
  - No effect for the non-Oracle users
- **Security mechanism on database level**
  - Works also when accessing with other applications
- **In production for Vegetable and Rice**

Acknowledge

- **IRRI**
  - Added multi-user functionalities in ICIS
- **Bayer Bioscience and Nunhems**
  - Collaborative work to set a common environment
- **ABIS**
  - Oracle consultant with VPD experience