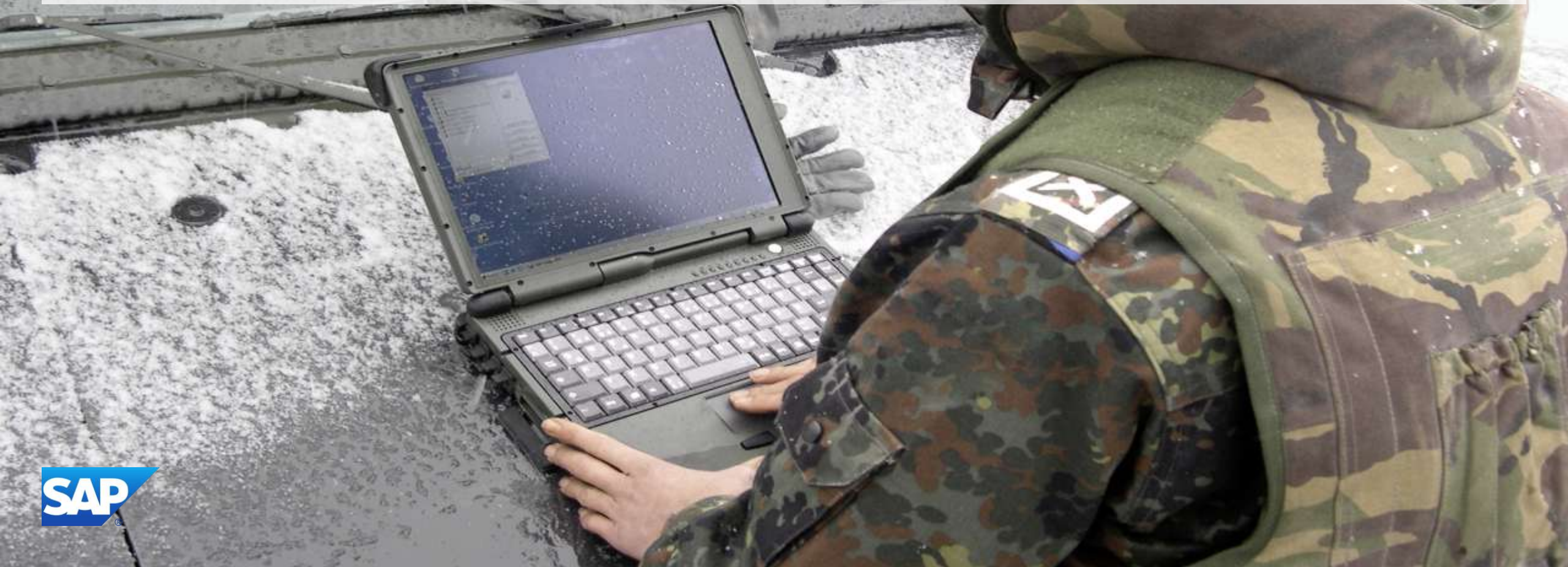
개인정보보호법에 대응하는 SAP 적용 방안

- UI Field Level Security by UI Masking and Access Logging

Kim, Sungwhan / SAP Consulting
Feb. 23, 2012



물관리 안한 20개 지자체 개발 올스톱

낙동·영산·금강 수계... 3월부터 공단·아파트·백화점 등 인허가 전면금지. 오염물질배출 제재법 첫 발동

광주광역시와 충북 청원군, 전남 나주시·담양군 등 낙동강·금강·영산강 수계(水系·물줄기)에 있는 전국 20개 지자체가 각 시도에 허용된 수질 오염물질 배출량 한도를 초과, 다음달부터 주요 개발사업의 인·허가가 전면 금지되는 제재를 받게 됐다. 금지되는 개발사업에는 도시개발과 산업·관광단지 개발, 공장·대학·아파트·백화점 건설 등이 포함된다.

환경부는 최근 이들 20개 지자체 관계자를 정부 과천청사로 불러 이 같은 방침을 공식 통보한 것으로 22일 확인됐다. 환경부 관계자는 "이달 중 국토해양부 등 정부부처와 광역단체장에게 '관련 법에 따라 이들 지자체에 대한 개발사업 인·허가를 금지해 달라'는 내용의 공문을 발송할 예정"이라고 말했다. 정부당국이 환경 관련 법을 어겨 지자체의 신규 개발사업을 사실상 전면 금지시키기는 이번이 처음이다.

이번 조치는 2002년 제정된 '3대강 수계 물관리 및 주민지원에 관한 법률'에 규정된 행정제재 조항을 환경부가 처음 발동하는 것이다.

이 법엔 3대강 수계에 속한 지자체들이 과도한 개발행위 등으로 수질 오염물질 배출허용량을 지키지 않을 경우 정부부처 등 인·허가권자는 산업단지·도시개발 등 각종 개발행위를 승인·허가하지 않도록 규정돼 있다. 서울·인천·경기 등 한강수계 지자체는 내년 6월 관련 법이 시행된다.

환경부 관계자는 "최근 3대강 수계 소속 68개 지자체의 '1단계 수질오염총량관리제(2006~2010년)' 시행 평가를 마무리한 결과 이 중 20개 지자체가 배출 허용량을 초과한 것으로 최종 확인됐다"고 말했다.

이들 지자체에 대한 개발사업 제재는 환경부가 관련 정부부처 등에 지자체 명단을 통보하는 순간부터 시작돼 각 지자체가 당초 허용된 오염물질 배출 허용량 수준 이하로 오염물질 배출을 줄일 때까지 계속된다.

(Source : 2012. 02. 23. 조선일보)

Field Level Security and UI Masking의 필요성 – 접근 통제

28 ( )
① . . .
 . .
1. .
2. .
3. .
4. .
5. .
6.
② .

28 2( )
① . .
② .

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 문서에 보면, 상기와 같이 개인정보가 누설 되지 않도록 **기술적, 관리적** 조치를 취하도록 되어 있음.
- DB 암호화를 기본적으로 구현하고, **사내 직원에 의한 정보 누설을 막기 위해 UI Masking / UI Logging 을 중심으로한 Field Level Security 구현** 또한 중요한 조치 사항임.

UI Masking Example from

9. 개인정보 표시제한 보호조치

제9조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인 정보를 마스킹하여 표시제한 조치를 취하는 경우에는 다음의 원칙으로 적용할 수 있다.

1. 성명 중 이름의 첫 번째 글자 이상
2. 생년월일
3. 전화번호 또는 휴대폰 전화번호의 국번
4. 주소의 읍 · 면 · 동
5. 인터넷주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

개인정보 표시제한 보호조치가 적용된 개인정보 조회 화면(예시)

성명	홍*동	생년월일	****년 *월 *일
전화번호	02-****-1234	핸드폰	010-****-1234
주소	서울 종로구 ***동 12-3	접속지 IP	123.123.***.123

개인정보 보호법 – 개인정보 안정성 확보

법률적 요구 사항

개인정보의 안전한 처리를위한

- 내부 관리계획의 수립 및 시행, 개인정보에 대한 **접근 통제** 및 **접근 권한**의 제한 조치,
- 개인정보를 안전하게 저장·전송할 수 있는 **암호화기술의 적용** 또는 이에 상응하는 조치,
- 개인정보 침해사고 발생에 대응하기 위한 **접속기록의 보관** 및 위변조 방지를 위한 조치,
- 개인정보에 대한 **보안 프로그램의 설치** 및 갱신,
- 개인 정보의 안전한 보관을 위한 보관시설 마련 또는 잠금장치의 설치 등 물리적 조치 등이다.

IT 요구 사항

- ✓ **DB Encryption**
- ✓ **DB Access Control**
- ✓ **UI Masking (SAP)**
- ✓ **Access Logging (SAP)**

Total Security including DB Encryption and Field Level Security

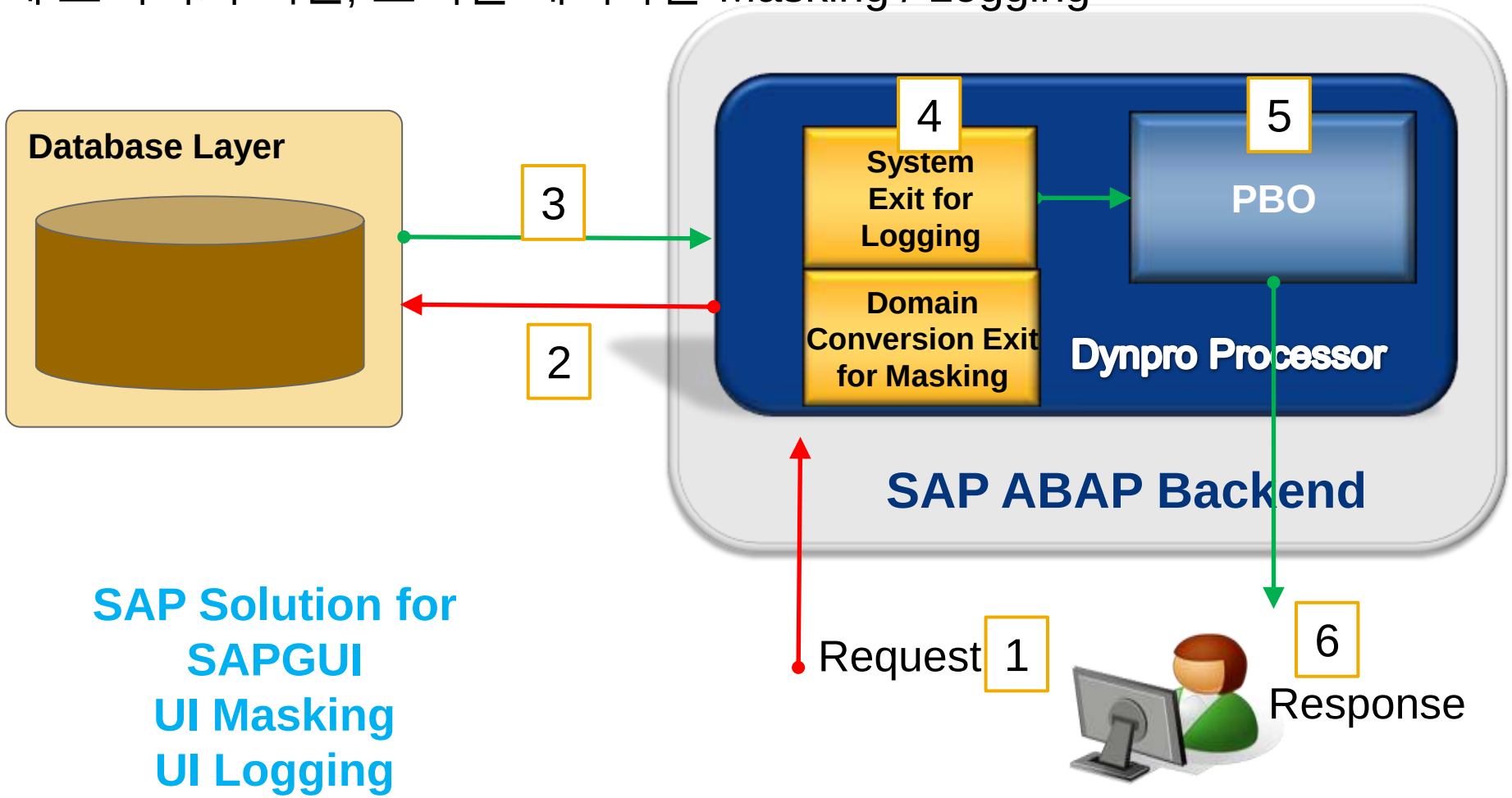
- Total Security를 위해 DB Encryption과 함께 UI Protection이 필요함.
- DB Encryption Solution으로 TDE (transparent Data Encryption) 를 비롯한 여러 3rd Party Solution 등을 고려할 수 있음. SAP는 이러한 솔루션에 중립임.

- UI Protection은 기본적으로 필드레벨 보안이 필요하나 Standard SAP security는 t-code 또는 table level 중심이기에 필드레벨 보안이 제한적임.

- **이에 SAP에서는 필드레벨의 보안 솔루션을 출시 하여 아래를 제공함**
  - Field Level UI Masking
  - Field Level Read Access Logging

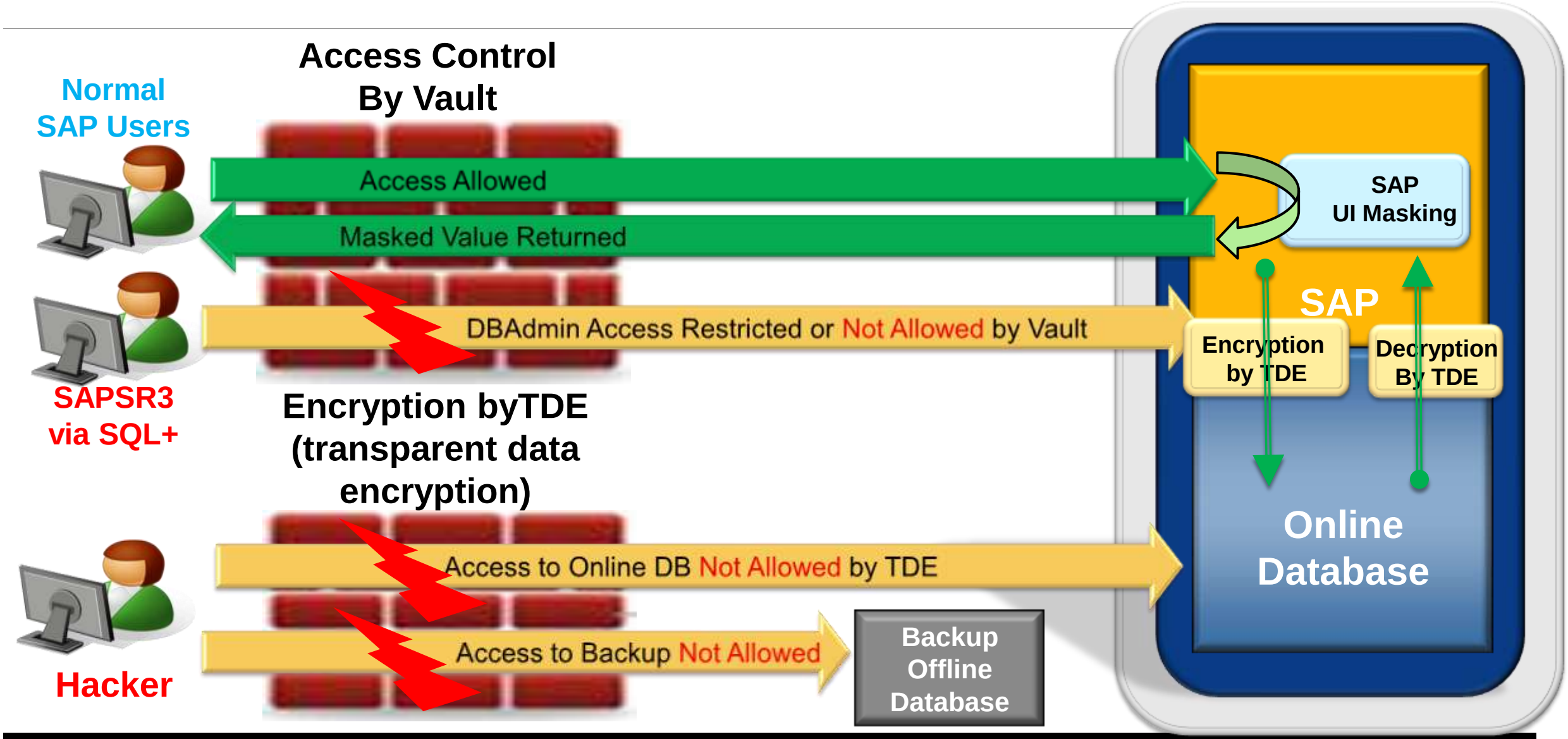
UI Masking / UI Logging Architecture

화면에 보여지기 직전, 보여질 데이타를 Masking / Logging



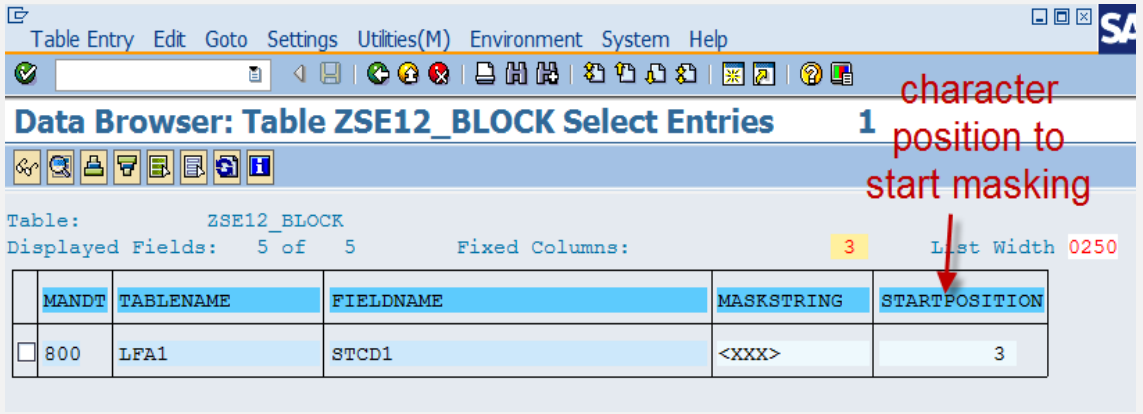
SAP Solution for
SAPGUI
UI Masking
UI Logging

Scenario Example: TDE / Vault / SAP UI Masking Combination



SAP UI Masking Solution

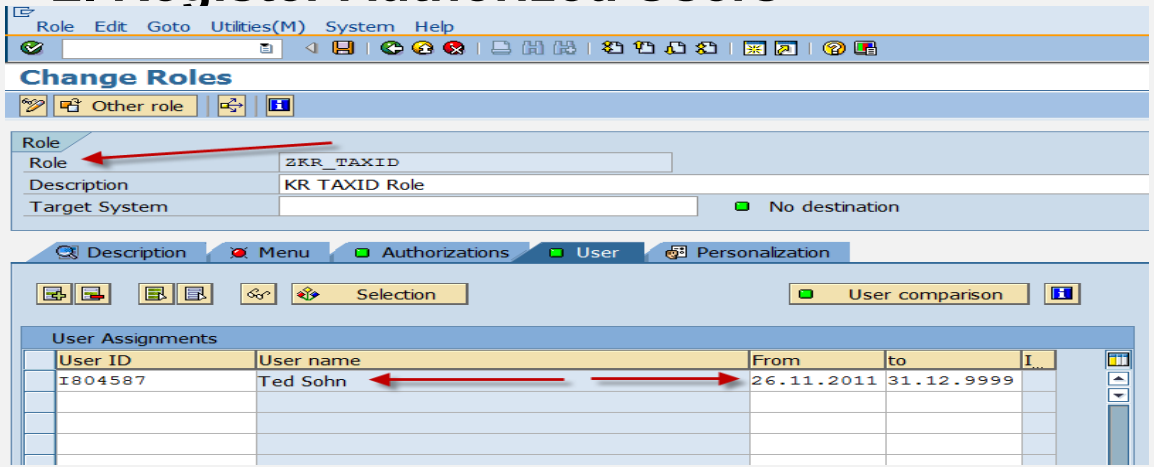
1. Define Masking Rules



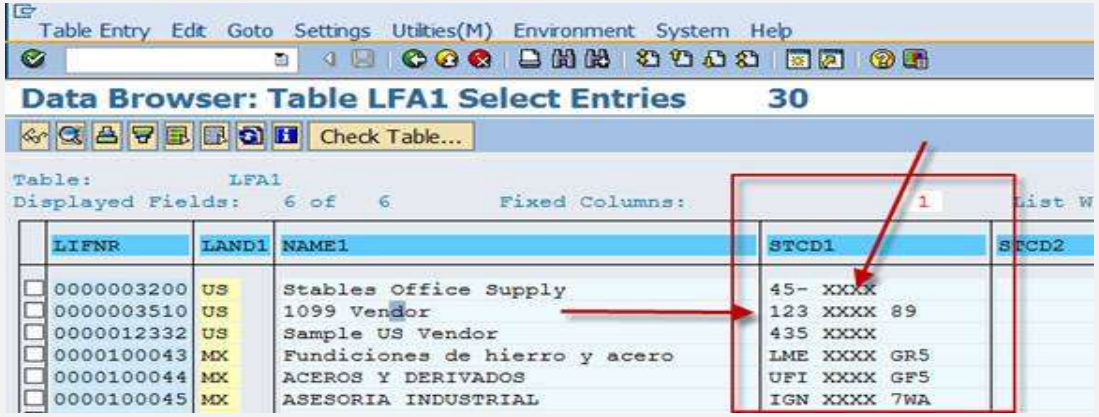
Easy To Use

1. Define Masking Rule(s) for each field
2. Register Authorized End Users for each field that should be protected
3. Authorized users for the field can see the original value in SAP GUI, but others not authorized will get masked value.

2. Register Authorized Users



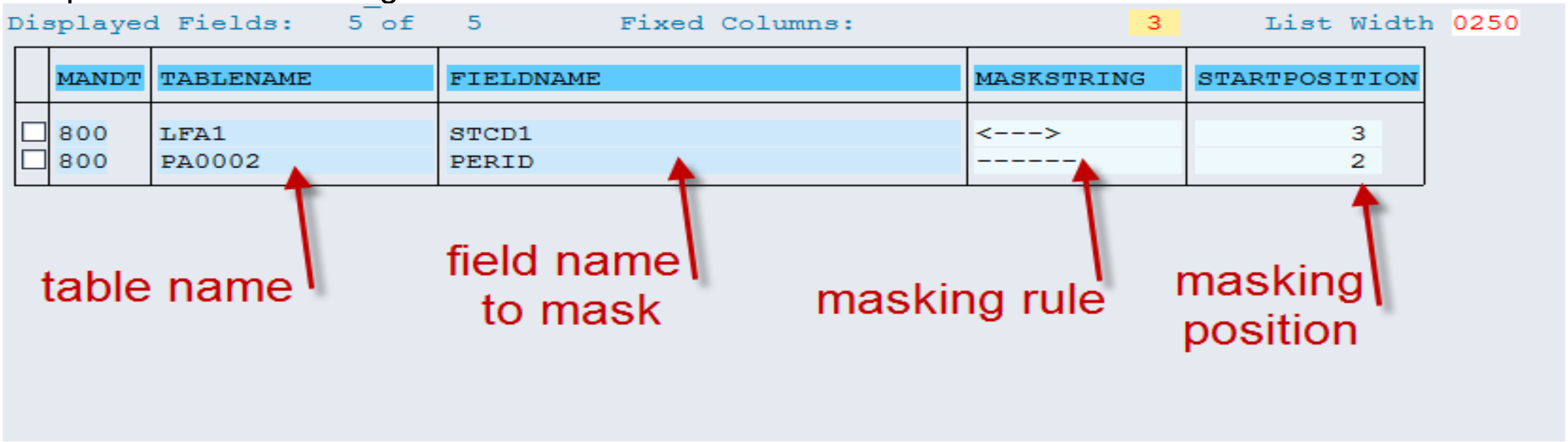
3. Result



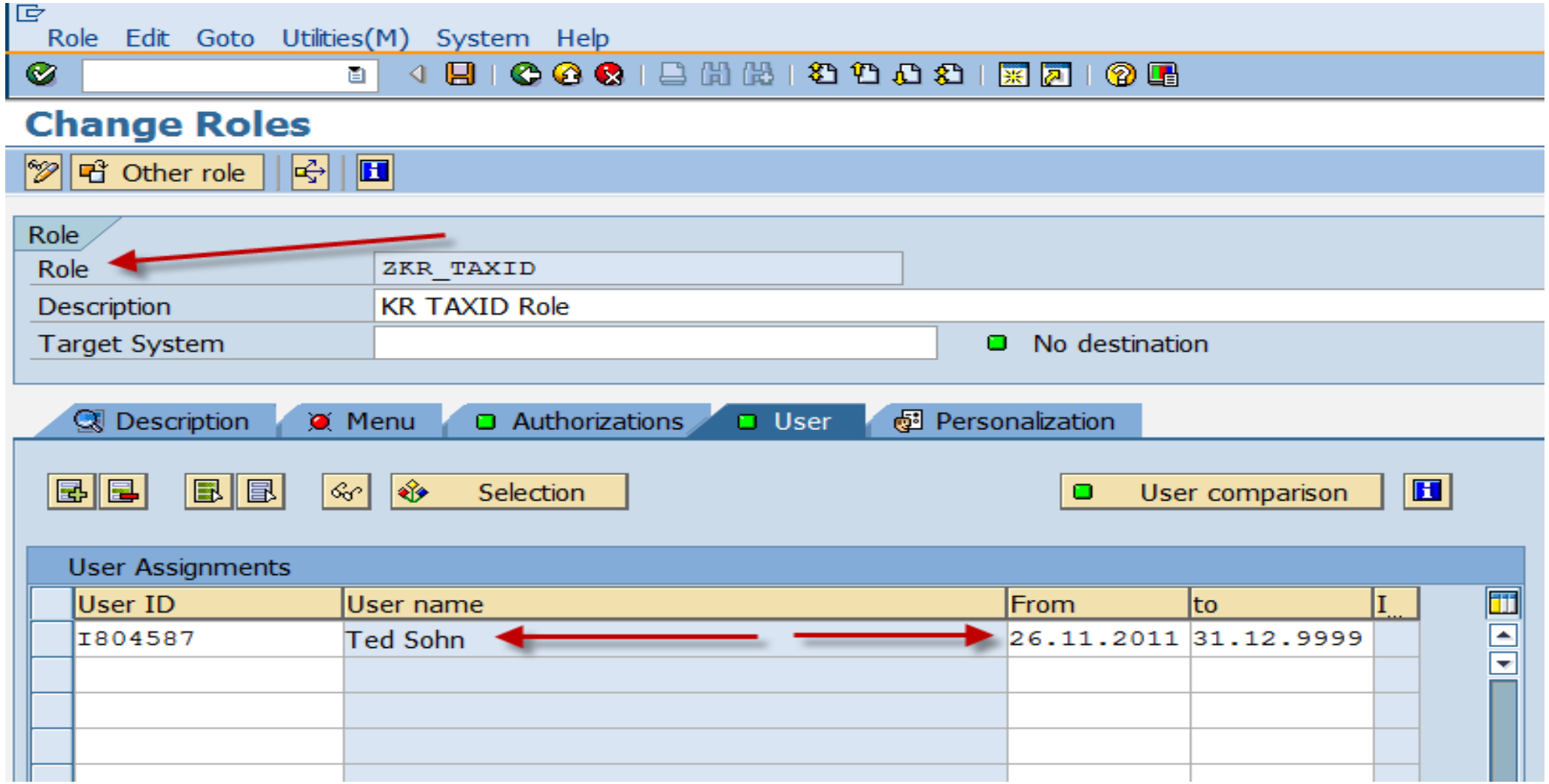
Step 1. Masking Fields & Masking Rules (sample from lab)

- Masking rule can be different by fields. Multiple Masking Rules Supported: for example, the first 1-3 characters by xxx and 5-6 characters by **

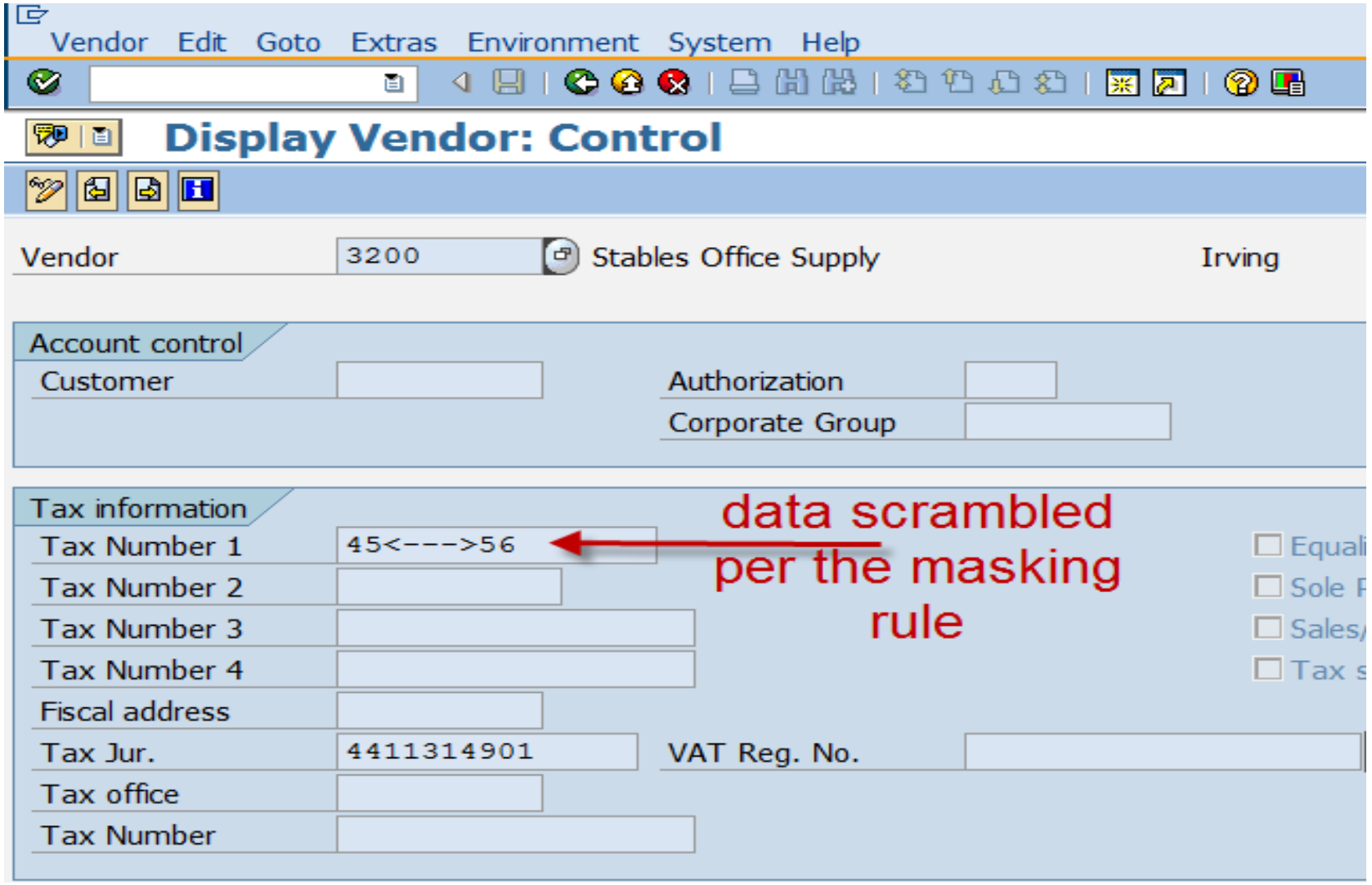
-- BADI for each field is delivered in the solution so that customers themselves can implement complicated business logic for each field.



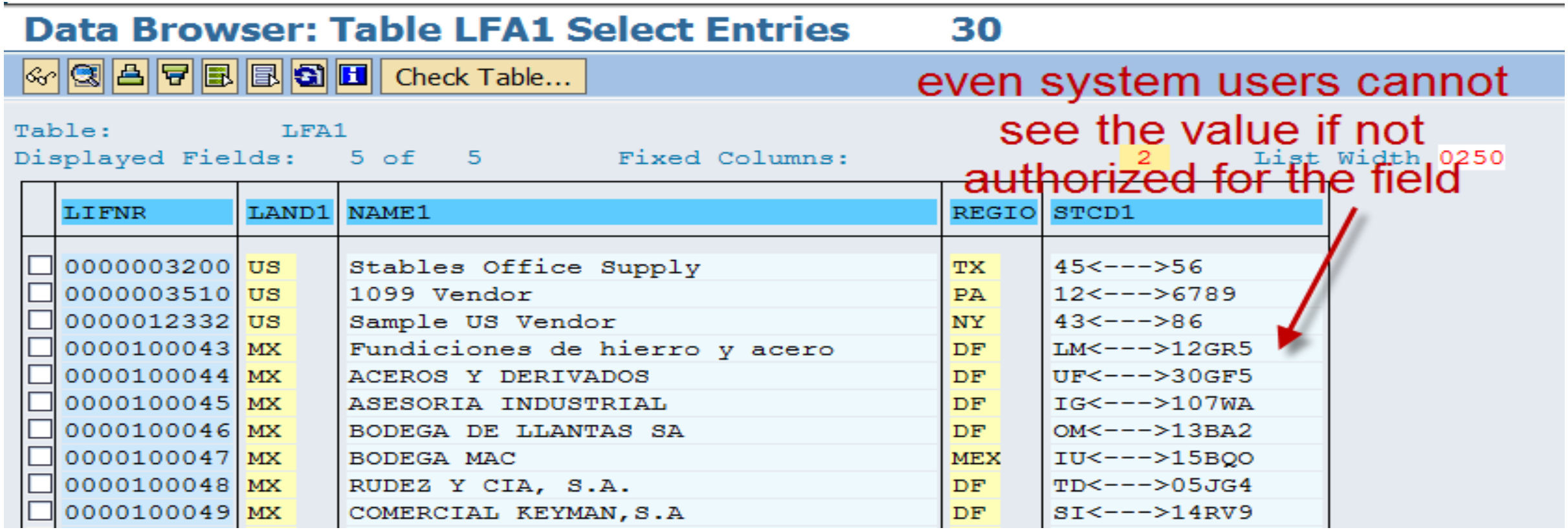
Step 2. Register Authorized End Users for Each Field



Sample Masking Result 1: End Users Not Authorized for the Field



Sample Masking Result 2: Even System Users cannot see if not authorized for the field: Applicable to SE11, SE12, SE16

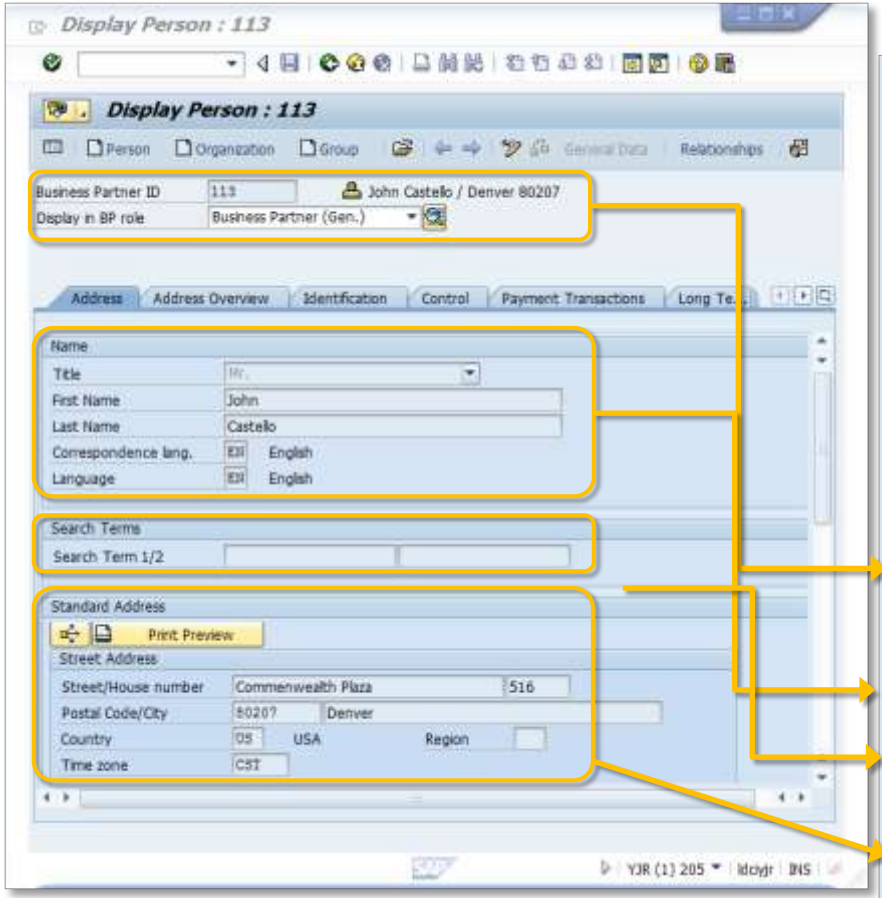


LIFNR	LAND1	NAME1	REGIO	STCD1
0000003200	US	Stables Office Supply	TX	45<--->56
0000003510	US	1099 Vendor	PA	12<--->6789
0000012332	US	Sample US Vendor	NY	43<--->86
0000100043	MX	Fundiciones de hierro y acero	DF	LM<--->12GR5
0000100044	MX	ACEROS Y DERIVADOS	DF	UF<--->30GF5
0000100045	MX	ASESORIA INDUSTRIAL	DF	IG<--->107WA
0000100046	MX	BODEGA DE LLANTAS SA	DF	OM<--->13BA2
0000100047	MX	BODEGA MAC	MEX	IU<--->15BQO
0000100048	MX	RUDEZ Y CIA, S.A.	DF	TD<--->05JG4
0000100049	MX	COMERCIAL KEYMAN,S.A	DF	SI<--->14RV9

SAP Read Access UI Logging Solution (screens from lab)

- If not masked in the display, then it will is recorded for audit trail.
- What will be logged?
  - Who – user ID
  - When - timestamp
  - From where (Client PC IP Address)
  - By which transaction
  - Which field
  - Which value

Transaction BP (Business Partner)



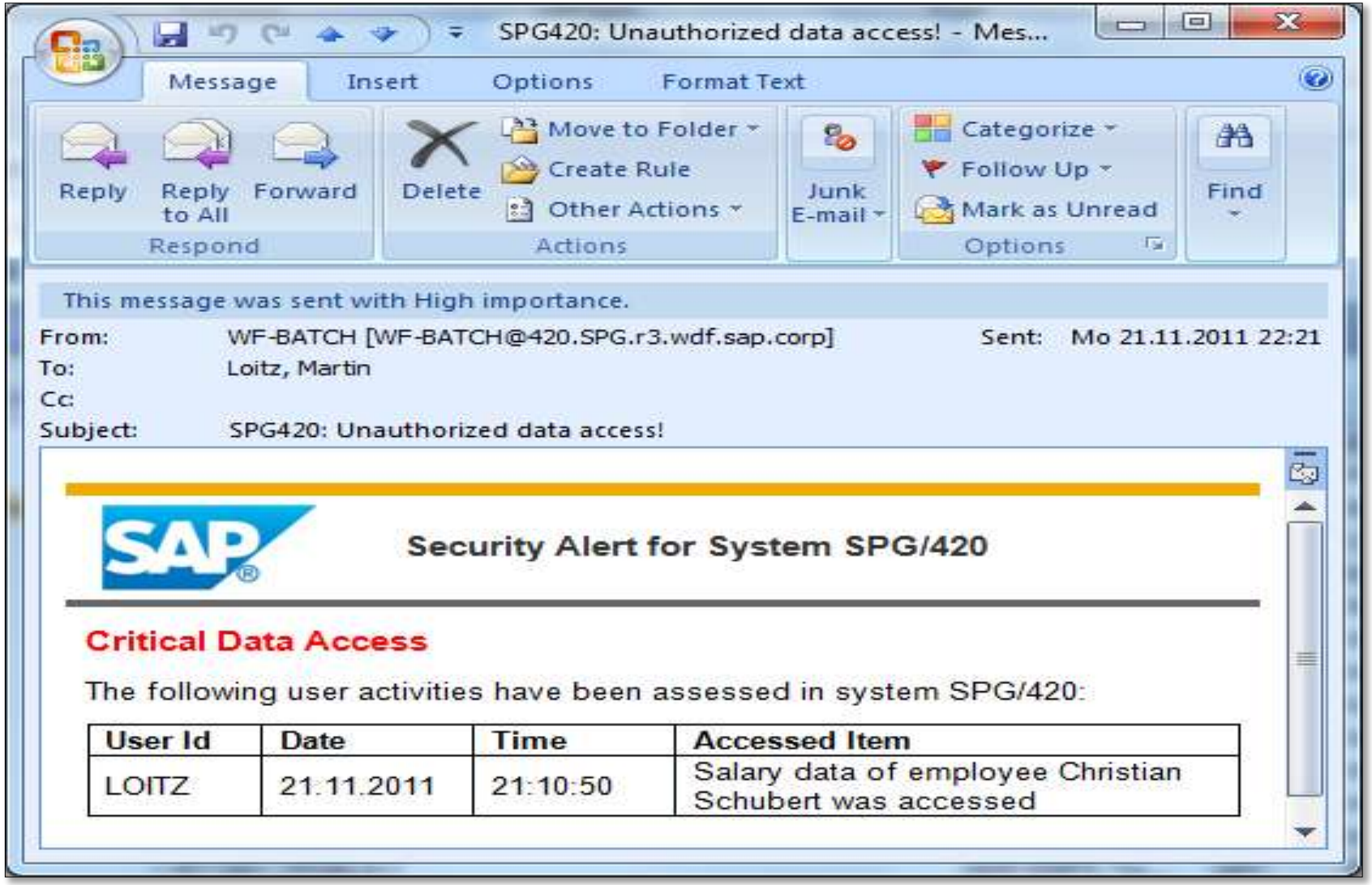
Sample Logging

```
**********************************************************************
**********                    HEADER                    **********
**********************************************************************
GUID=005056A505DF1EE0ACA917F573568FC4;
TIMESTAMP=18.07.2011 16:18:03;
TRX_NAME=BP-Maintain Business Partner;
USERNAME=MILLERJOHN;
CLIENT_PC=10.18.161.143;
PROCESS_STATUS=00;
TECHNOLOGY=10;

**********************************************************************
**********                    INPUT                     **********
**********************************************************************
SAP_SYSTEM=YJR;
SAP_CLIENT=205;
TITLE=Display Person : 113;
Function code that PAI triggered=;

**********************************************************************
**********                    OUTPUT                    **********
**********************************************************************
SAP_SYSTEM=YJR;
SAP_CLIENT=205;
TITLE=Display Person : 113;
BP.SAPLBUS_LOCATOR.3000.SAPLBUPA_DIALOG_JOEL.1510.BUS_JOEL_MAIN.CHANGE_NU
BP.SAPLBUS_LOCATOR.3000.SAPLBUPA_DIALOG_JOEL.1510.BUS_JOEL_MAIN.PARTNER_T
BP.SAPLBUS_LOCATOR.3000.SAPLBUPA_DIALOG_JOEL.1510.BUS_JOEL_MAIN.CHANGE_DE
BP.SAPLBUS_LOCATOR.3000.SAPLBUPA_DIALOG_JOEL.1110.BUS_JOEL_MAIN.PARTNER_R
BP.SAPLBUS_LOCATOR.3000.SAPLBUPA_DIALOG_JOEL.1110.BUS_JOEL_MAIN.PARTNER_R
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1130.BUS000FLDS.TITLE_MEDI[0]()=0002;
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1301.BUT000.NAME_FIRST[0]()=John;
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1302.BUT000.NAME_LAST[0]()=Castello;
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1360.BUS000FLDS.LANGUCORR[0]()=EN;
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1360.BUS000FLDS.LANGU_CORR[0]()=English;
BP.SAPLBUS_LOCATOR.3000.SAPLBUD0.1135.BUS000FLDS.LANGU[0]()=EN;
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_KEYW.STREET[0]()=Street/House n
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_DATA.STREET[0]()=Commenwealth
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_DATA.HOUSE_NUM1[0]()=516;
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.G_CITY_POSTCODE1_LABEL[0]()=Postal Co
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_DATA.POST_CODE1[0]()=80207;
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_DATA.CITY1[0]()=Denver;
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.ADDR2_DATA.COUNTRY[0]()=US;
BP.SAPLBUS_LOCATOR.3000.SAPLSZA7.0601.T005T.LANDX[0]()=USA;
```

SAP Read Access UI Logging Solution:
Can trigger workflow via BADI (screens from lab)



*** Not part of solution**

Summary: SAP UI Masking / Logging Features

- SAP UI Masking / Logging brings , “Preventive” protection

SAP UI Masking / Access Logging	
Solution by	SAP standard solution
Certification	Supported, maintained by SAP
API or Configuration	SAP Configuration based solution -Easy to use -Easy to maintain
Modification or Configuration	Only Configuration Needed -Easy to upgrade, Easy to reset, Easy to reconfigure -Easy implementation -SAP responsible for any upgrade issue
Custom Logic	Can be integrated with other SAP tools -BADI is provided by default for each field -Custom logic can be added by BADI
Performance	No performance concern at all No search concern at all
예방적 효과 Preventive Effect	Powerful UI Logging UI Logging brings “Preventive” security effect.

Summary: SAP UI Masking / Logging Features

내부 직원에 의한 개인정보 누출 차단

- 필드 레벨에서의 차별적 시큐러티 솔루션
- End-User 뿐만 아니라, Admin-User에 대해서도 Protection
- 원하는 필드에 대한 Flexible한 설정

UI 마스킹은 SAP Standard UI 와 CBO UI 에 함께 적용

- 마스크할 필드를 등록하면 그 필드를 쓰는 모든 UI (standard plus CBO) 에 마스킹 함께 적용.
- 프로그램 (Standard, CBO)변경없이 Configuration 으로 적용 가능

유연하고, 확장가능한 솔루션 지원, can work with any DB Encryption Solution

- UI Masking 과 함께 필드레벨에서의 UI logging 제공
- Irrelevant to the database encryption in place / Not Affected by Database Encryption Solution

검증된 품질관리 / 성능 이슈 없음

- SAP 솔루션은 성능에 영향 주지 않음.
- 사용 및 관리 용이. No Special User Training Needed.
- **약 1.5개월 정도의 짧은 적용 기간.**

Security Best Practice & Health Check Service is also available

- Total Security Review, Governance Review, Evaluation, Assessment Service

Thank You!

상세한 내용은 담당영업대표께 문의 바랍니다.

김 성 환
Client Partner / Director
SAP Consulting / SAP Korea
Sung.whan.kim@SAP.com
010 3227 9416