

# RCS UI Field Security (UI Masking)

Tobias Keller, Product Owner  
Custom Development, SAP SE  
December 2014

The SAP logo is located in the bottom left corner of the slide. It consists of the letters 'SAP' in a bold, white, sans-serif font, set against a blue rectangular background with a white diagonal line.

# Data Security

## The insider threat

**Vodafone Australia sacks employees over data leak**


Friday 14 January 2011 11:44

Vodafone Australia has sacked several people after four million customer records were exposed in a privacy leak.

Vodafone employees allegedly sold private customer details and records with access to entire lists of calls and messages from individuals.

Company employees have been accused of selling the sensitive information to criminal gangs. The firm said it is reviewing its IT systems security, processes and training.

Vodafone Australia chief executive, Nigel Dews, said, "We've made swift progress. We've terminated the employment of a number of staff; we've undertaken a review of the security systems and processes, and we're implementing some of the initiatives."



**Insider Data Theft Among Top Cybersecurity Threats for US Federal Agencies: Study**

Breaches were blamed on "careless and untrained insiders" in 42 percent of cases.


**Forrester report finds most data breaches are caused by employees**

By John E. Dunn, Computerworld UK

Sep 24, 2012 1:40 PM

Most data breaches are caused by mundane events such as employees losing, having stolen or simply unwittingly misusing corporate assets, a Forrester Research report has found.


After questioning over 7,000 IT executives and ordinary employees across North America and Europe, 31 percent cited



**Uni-Klinik sperrt Personalakte von Michael Schumacher**

Die Uni-Klinik in Grenoble hat offenbar die Patientenakte von Michael Schumacher gesperrt. Die medizinische Leitung hat sich laut Medienberichten zu diesem Schritt entschlossen, da sich zahlreiche unbefugte Mitarbeiter über einen Computer Zugang zu den Dokumenten verschafft haben sollen.

Von GMX Redaktionsmitglied Tim Frische



**Ex-employees are likely cause of data leakage**

Often motivated by feelings of ill will, some workers may decide to steal sensitive company data and bring it out with them on their last day within an organization. This kind of data leakage happens more often than one may think, and it often goes unreported and unrecognized until administrators see their sensitive data outside their own company.

A recent Ponemon Institute survey showed that 50 percent of participants admitted to sensitive information with them when leaving a position, stated The Wall Street Journal. Robert Yonowitz, a partner with law firm Fisher & Phillips LLP, told Network World that issues relating to ex-employee data leakage occur within the first two weeks after a worker leaves their position. Businesses need to proactively address this issue in order to ensure that essential, sensitive data.

**The Economist** ...insiders bent on leaking sensitive data can cause huge damage. This can involve large sums of money [...]. Almost half [cases researched] involved losses of more than \$1m.

**Employees, not hackers, cause most corporate data loss**

Much security coverage focuses on malware, hackers, and the dangers both pose ...

by Joel Hruska - Oct 12 2008, 8:30pm WEDT

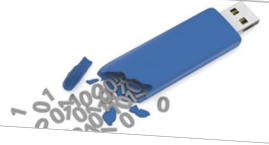
Earlier this summer, we covered a report suggesting that the majority of corporate data loss comes from risky employee actions and systemic failures at the corporate level when it comes to implementing comprehensive IT security policies. Now, a new study from Compuware reports new information that supports Trend Micro's conclusions from back in July. The unsung heroes in the IT department, it turns out, may be doing a better job stopping outside hackers than they get credit for.

**Employees are the biggest threat to cyber security, says report**

By Danny Palmer

15 Jul 2013

1 Comment



Newsletters

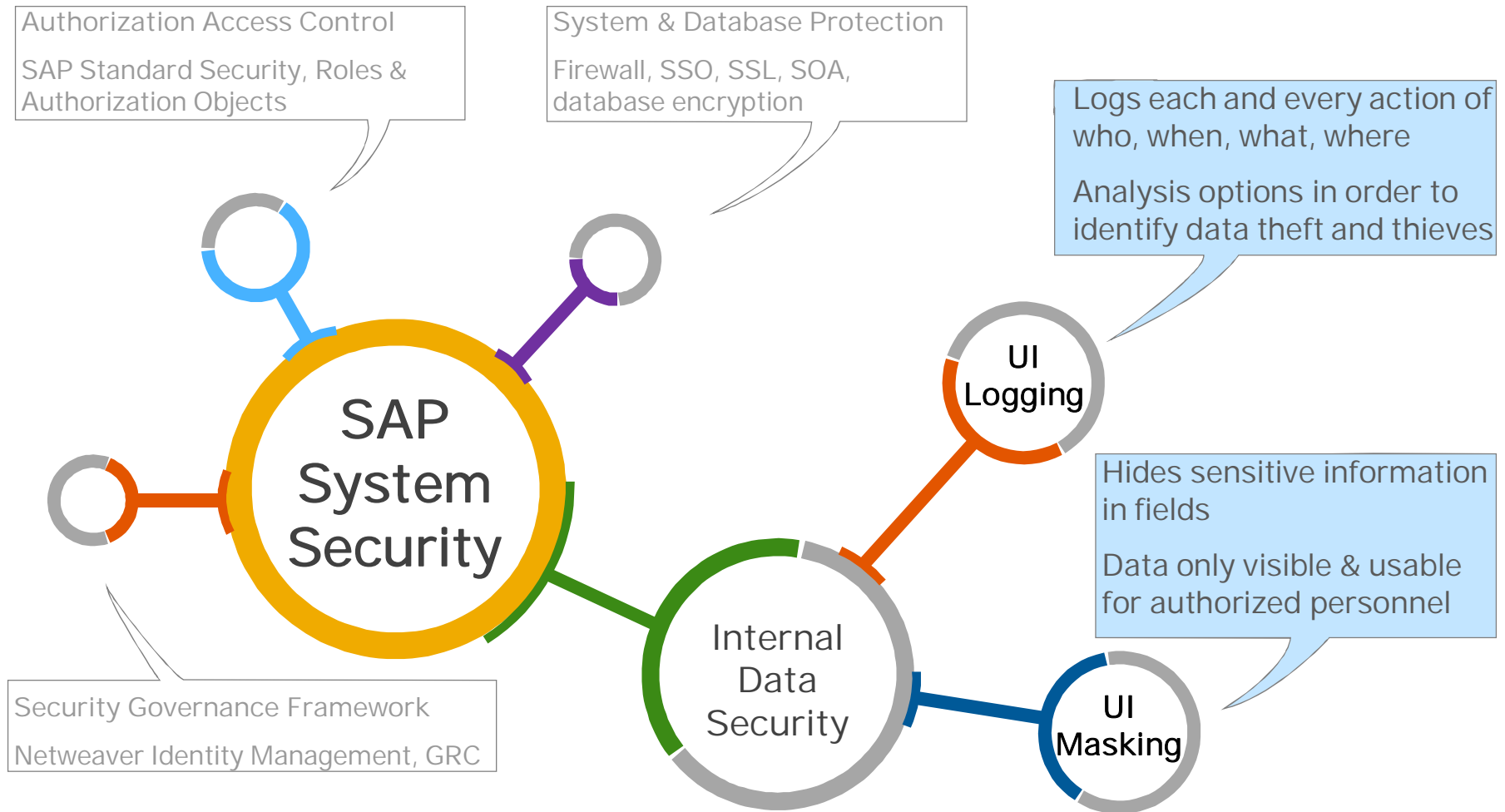
Sign up for our FREE newsletters:

- > Daily update
- > Weekly update

Sign up

# Data Security

## SAP system security: technical components



# RCS UI Masking

## Elevator Pitch

---

### What is UI Masking?

- active form of suppressing display of sensitive data in SAP GUI
- logging of requests to access configured data fields

### How does it work?

- technically mask sensitive data before being displayed
- configure which (and how) data is masked
- configure who (role/user) is authorized to see unmasked data
- tracking of requests for sensitive data (who, when, what, IP address...) with archiving the for log file

### What do I get from this?

- avoid damaging and costly cases of data loss
- ensure compliance with data privacy regulations
- increase transparency of access to sensitive data with audit trail on field level.

# RCS UI Masking & UI Logging

## Distinction

### UI Masking

Use case: sensible data should be concealed from specific users/roles

Strong approach to data security

- technically prevent employees from accessing sensitive data

Pro-active approach

- technically rendering selected information unusable in selected users' interfaces
- prevent opportunistic leaking of data

Build human firewall and empower employees

- Raise data security awareness
- Protect employees against inadvertent data security breaches
- Increase employees to confidently do their work

### UI Logging

Use case: Sensible data must remain generally accessible

Soft approach to data security

- Deter opportunistic security breaches

Retroactive approach (hygiene factor)

- Enable uncovering and sanctioning of offenders (after the fact)
- Clear blameless suspects' names

Build "human firewall"

- Communicate technical logging ability as well as handling and sanctioning of data security incidents
- Raise awareness for data security
- Build trust among employees (and customers) that their data are adequately protected



# RCS UI Logging / UI Field Security

## Value Drivers

---

### Decrease risk

- protect your enterprise against damaging disclosure of internal, secret, or otherwise sensitive data
- ensure compliance with data privacy regulations
- protect your enterprise against litigation (e.g. violation of personal rights) and fines
- increase transparency of access to sensitive data
- increase awareness of employees to data protection (“human firewall”)

### Maintain credibility

- towards market/customers
- towards employees

# RCS UI Masking

## Unique Selling Proposition

---

- Benefits from **deep technical integration** into SAP ERP/Netweaver (which can only be realized by SAP as software provider):
  - Non-modifying approach (SP2, released December 2014), completely configurable, generically usable across SAP GUI
  - Resource efficient data masking functionality on server-side
  - Customer specific logic what/how to mask can be introduced via BADIs during implementation without modification
  - Integration into ERP native authorization/role concept
- **Increased protection**
  - Augments and reinforces existing data security measures, e.g. authorization concept, UI Logging, etc.
  - Transparent data usage by means of tracing all or “unmasked” data requests
  - Mask data also in mass access transactions (SE16, SE16n, SE11) and functionality (download, export, print), partly by hiding sensitive information, or suppressing menu functions
- **Efficient installation and implementation**
  - Quick installation of the required add-on with SAINT
  - Rapid configuration after identification of sensitive fields
  - Configuration is transportable to other clients/systems via transport structure
- Product team can provide **further customer requirements on request**

→ UI Masking is unique in the market considering the overall offering out of functionality, security and integration depth.

# RCS UI Masking Configuration

## 1. Define fields to be masked, and rules

- Define which field are masked.
- Configure on field level how a field is displayed. Define for up to three segments whether data are shown, or how they are masked.
- UIM also provides a BADI for implementing complex business logic.

## 2. Register Authorized Users per Field

- In transaction PFCG, assign users to the UI Masking authorization a role.
- Users assigned to these roles will be able to see unmasked values for the applicable fields

The image shows two SAP screenshots. The left screenshot is 'Maintain Masking Configuration' with a table of field configurations. The right screenshot is 'Change Roles' showing role configuration and user assignments.

Table Name	Field Name	HR Relev.	Set1 From	Masking character – set 1	Set2 From	M...	Set3 From	M...	Mask Ctrl.	UI Log
PA0006	LOCAI	<input checked="" type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always
PA0006	TELNK	<input checked="" type="checkbox"/>	1	#####					<input checked="" type="checkbox"/>	Always
PA0008	ANSAL	<input type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always
Q0002	FATXI	<input type="checkbox"/>	1	**					<input checked="" type="checkbox"/>	Always
Q0008	ANSAL	<input type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always
Q0008	BETRQ	<input type="checkbox"/>	1	*****					<input type="checkbox"/>	Always_ ZABC
Q0009	EMFTX	<input type="checkbox"/>	2	\$\$	3	##			<input type="checkbox"/>	Always_ ZABC
RESBD	MATXI	<input type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always_ ZPR_
RESBD	POSNR	<input type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always_ ZPR_
RESBD	POTX1	<input type="checkbox"/>	1	*****					<input checked="" type="checkbox"/>	Always_ ZPR_

The right screenshot shows the 'Change Roles' transaction for role 'ZKR\_TAXID'. The role description is 'KR TAXID Role' and the target system is 'No destination'. Below, the 'User Assignments' table shows user 'Ted Sohn' (User ID 1804587) assigned to the role from 26.11.2011 to 31.12.9999.



# RCS UI Masking

## Masking result

### 3. Result: data masking

Data is masked in GUI transaction display for un-authorized users.

This also affects high-level "admin" system users (in dynamic transactions, e.g. SE11, SE12, SE16, SE16n) unless explicitly authorized

UI Masking also protects data during download, export, and print

Display Vendor: Control

Vendor: 3200 Stables Office Supply Irving

Account control: Customer, Authorization, Corporate Group

Tax information: Tax Number 1: 45<--->56, Tax Number 2, Tax Number 3

Data Browser: Table LFA1 Select Entries

LIFNR	LAND1	NAME1	REGIO	STCD1
000003200	US	Stables Office Supply	TX	45<--->56
000003510	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

Annotations: "data scrambled per the masking rule" points to the masked tax numbers. "even system users cannot see the value if not authorized for the field" points to the masked STCD1 values in the table.

ted mask1.txt - Notepad

Table: LFA1  
Displayed Fields: 4 of 4 Fixed Columns: 2

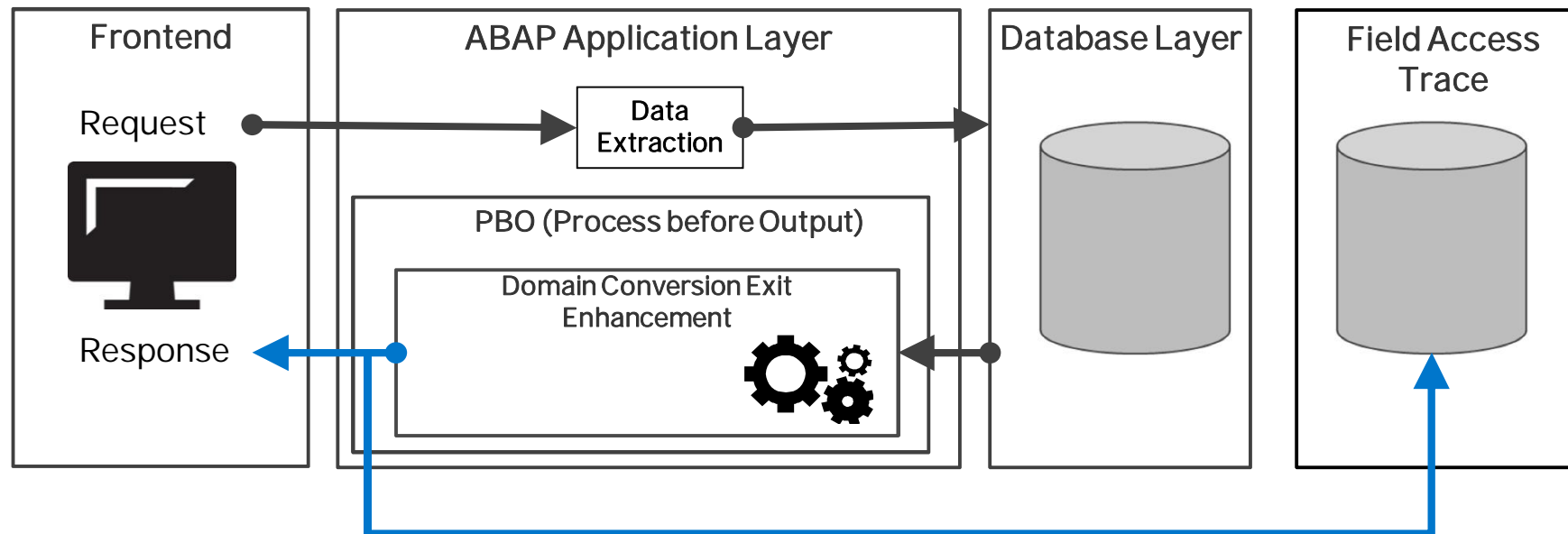
LIFNR	LAND1	NAME1	STCD1
1<*****>789			1<*****>789
4<*****>6			4<*****>6
L<*****>2GR5			L<*****>2GR5
U<*****>0GF5			U<*****>0GF5
I<*****>07WA			I<*****>07WA
O<*****>3BA2			O<*****>3BA2
T<*****>5000			T<*****>5000

Annotations: A red arrow points to the masked STCD1 column header in the table view.

# RCS UI Masking

## Technical Details: High level solution architecture (SP1)

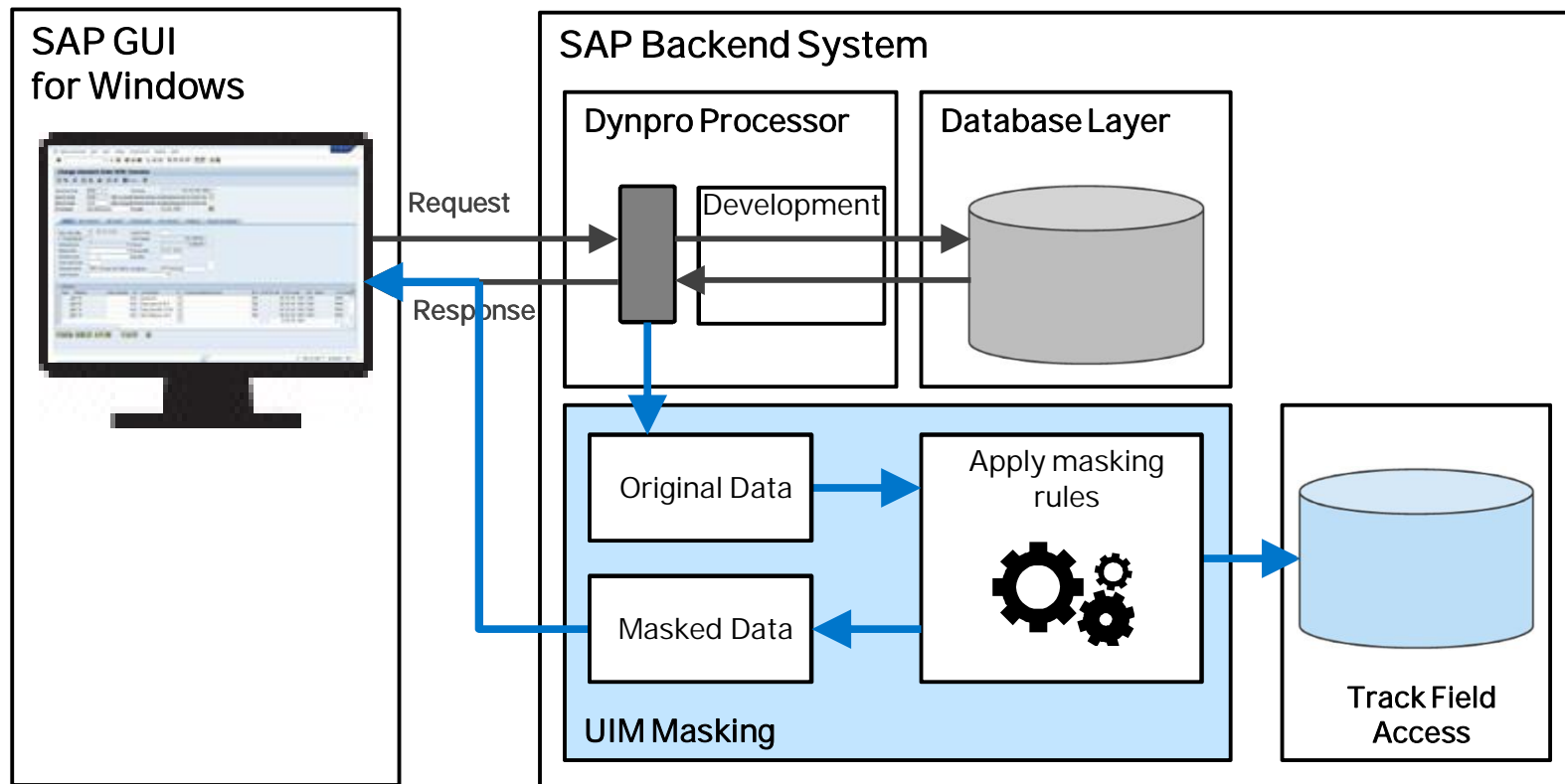
UI Masking masks (and logs) data immediately before displaying in a SAP GUI screen (no data are altered on database level)



# RCS UI Masking

## Technical Details: High level solution architecture (SP2)

UI Masking identifies data to be masked and applies the masking rules immediately before displaying in a SAP GUI screen. No data are altered on database level.



# RCS UI Masking

## Functional scope & highlights

---

- Multiple masking rules, configurable on field level
- Masking will also be conducted for download and printouts
- BADI can be implemented with complex business logic for masking data
- Access tracking: generates an audit trail, configurable on field level
- Archiving functionality for the tracking file
- minimal/no impact on system performance
- integration into SAP native roles
- supports SAP GUI for Windows, Java, HMTL as well as NW BC

# RCS UI Masking

## Functional scope (1)

---

- Solution provides configurability for the following major functions on field level:
  - **masking scope** – fields that are subject to protection through masking
  - **masking patterns and characters** (alternatively: positions of masking characters)
  - **masking activation** (on field level, or through system wide switch)
  - **user role** required for access to unmasked data (can be assigned in Profile Generator PFCG)
  - **FAT (Field Access Tracking) activation** (always; never; data shown unmasked)  
In addition, BADI is provided for customer specific business logic on field level (overriding masking/FAT configuration)
- UI Field Security supports **content masking** for the following **SAPGUI** screens:
  - Dynpro Screens
  - ALV Grids
  - ALV List
  - technical transactions (e.g., SE16)

# RCS UI Masking

## Functional scope (2)

---

- In case of ALV grids, lists and technical transactions, **cell and column level masking** is possible.
- **Screen elements** can be of type Input; Output; Step Loops; Table controls
- **Data types** supported are CHAR, LCHR, LANG, LRAW, NUMC, RSTR, SSTR, STRG, VARC, CURR, QUAN, DATS, INT1, INT2, INT4.
- In display mode, data will be **masked**. In change mode, data will be masked and rendered as read-only. In “create” transactions, if masking is active for a field not prepopulated (to be entered by the user), saving will not be allowed.
- Data will appear **masked also in downloaded and printed content**.
- Configuration and BADI coding is organized in customization/workbench **transport requests for migration to other SAP systems/clients**.



# RCS UI Masking

## SP2 vs. SP1

---

### UIFS SP2 removes the following restrictions from SP1:

- Primary key fields can be masked in SP2
- Fields with foreign key relationship can be masked
- Multiple currency and quantity fields are supported in SP2 without loss of formatting
- Fields with standard conversion exits can be masked

### UIFS SP1 and SP2 work seamlessly side by side:

- SP2 natively supports the technical approach of SP1 (conversion exits)
- On screen field level, both a SP1 conversion exit and a SP2 Dynpro hook point can be configured. At runtime, the configuration executed first takes precedence (caution: a hook point BADI might not be executed in case a conversion exit performs masking first).
- SP1 conversion exits are supported, and are recommended for the time being for certain elements where no hook points are available (e.g. ADOBE forms).

# RCS UI Masking

## SAP Offering (UI Masking channels)

---

### **Supported UI technologies:**

- Masking in SAP GUI for Windows / HTML / Java

### **Supported SAP NetWeaver releases**

NW 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 on Hana

**RCS specific maintenance** (integrated into Standard maintenance)

Further enhancements and adaptations can be delivered **on request** (interface technologies, releases, customer specific functionality)

# RCS UI Masking

## Implementation – example

---

- **Installation of UIM add-on**
  - conducted by customer (ERP/basis team)
- **Implementation (configuration)**
  - Rule of thumb: 15-20 PD pure configuration effort for 10 transactions (consultant on-site, maintenance team offsite)
  - This excludes complex business logic (BADI implementation) and additional custom development)
- **Customer enablement**
  - The implementation also aims at enabling an in-house resource to handle the main parts of the execution phase of the implementation, and follow-up system changes.

# Contact – RCS UI Masking



Contact us at:

[uimasking@sap.com](mailto:uimasking@sap.com)

Visit our SAP UI Logging channel on SCN:  
<http://scn.sap.com/community/ui-logging>

Your one-shop-stop for product information,  
release news, Q&A, and more



Bharathi Srinivasa  
Technical Product Owner

SAP SE, Custom Development

T +91 804 139 83 22

E [bharathi.srinivasa@sap.com](mailto:bharathi.srinivasa@sap.com)  
[www.sap.com](http://www.sap.com)



Tobias Keller  
Product Owner

SAP SE, Custom Development  
Dietmar-Hopp-Allee 16  
69190 Walldorf

T +49 6227-7-74995

E [tobias.keller@sap.com](mailto:tobias.keller@sap.com)  
[www.sap.com](http://www.sap.com)

# © 2014 SAP SE

## All rights reserved.

---

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.