RCS UI Field Security (UI Masking)

Tobias Keller, Product Owner
Custom Development, SAP SE
December 2014
Data Security
The insider threat

Employees, not hackers, cause most corporate data loss

Much security coverage focuses on malware, hackers, and the dangers they pose...
Data Security
SAP system security: technical components

- Authorization Access Control
  SAP Standard Security, Roles & Authorization Objects
- System & Database Protection
  Firewall, SSO, SSL, SOA, database encryption

- Logs each and every action of who, when, what, where
  Analysis options in order to identify data theft and thieves

- Hides sensitive information in fields
  Data only visible & usable for authorized personnel

- Security Governance Framework
  Netweaver Identity Management, GRC

- Internal Data Security

- UI Masking

- UI Logging
  System & Database Protection
  Firewall, SSO, SSL, SOA, database encryption

© 2014 SAP SE. All rights reserved.
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):
  o Non-modifying approach (SP2, released December 2014), completely configurable, generically usable across SAP GUI
  o Resource efficient data masking functionality on server-side
  o Customer specific logic what/how to mask can be introduced via BADIs during implementation without modification
  o Integration into ERP native authorization/role concept
• Increased protection
  o Augments and reinforces existing data security measures, e.g. authorization concept, UI Logging, etc.
  o Transparent data usage by means of tracing all or “unmasked” data requests
  o 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
  o Quick installation of the required add-on with SAINT
  o Rapid configuration after identification of sensitive fields
  o 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
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.
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, HTML 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.