Dynamic Context Aware Data Protection
Tobias Keller, Product Manager, SAP
ASUG83699
About the Speaker

Tobias Keller

• Product Manager UI Data Security, SAP
• Based out of Walldorf, joining SAP 2007 as consultant and later solution architect in SD/mobility/usability; managing UI Masking and UI Logging solutions since 2013
Key Outcomes/Objectives

ABAC (Attribute Based Access Control) – authorizations for the smart enterprise!

1. New Generation access rights get more dynamic, based on the context of a request
2. Required “context” resides in SAP systems – waiting to be leveraged!
3. “attribute-policy” paradigm exemplified in “UI Data Security Masking for SAP S/4HANA” (UI Masking)
Agenda

- Business use cases
- Background on UI Masking
- Demo of attribute based access
- Q&A
Business Background
Temporary situation of “two organizations in one IT system” (M&A or spin-off)
If parts of an organization are split off (e.g. sold to another organization), processes and IT base usually take time to split. To avoid users from one entity also accessing the other organization’s HR data, pricing information, sales documents, etc., a logical split of the system needs to be conducted:
Context dependent access: legal restrictions from moving data outside a locality (offshore)

New legislation restricts users of a “foreign” locality to access specific information on “home” employees

Hypothetical Example: PII (personally identifying information) pertaining to U based employees may not be accessed by users based outside of the US (such as HR personnel in Europe, or IT support personnel in India)
Dynamic authorizations based on context and policies

Example based on implementation in UI Masking
UI Masking in the SAP security product portfolio

Embed GRC and security in SAP S/4HANA

- UI masking for SAP [ECC; SAP S/4HANA]
- UI logging for SAP [ECC, SAP S/4HANA]*
- SAP Enterprise Threat Detection*
- SAP Fortify by Micro Focus
- SAP Data Privacy Governance
- SAP Data Custodian
- SAP NetWeaver AS, add-on for code vulnerability analysis

*ISS security suite
UI Masking: data protection by configurable obfuscation of sensitive data in SAP UIs

- configurable scope of data to be protected
- configurable way how protection is required (security actions)
- configurable additional authorizations for “clear” access
  - roles
  - attributes and rules ("policies")

→ configurations evaluated at runtime
→ security actions applied to the UI layer only
UI Masking: data protection by configurable obfuscation of sensitive data in SAP UIs
Architectural Overview UI Masking

SAP S/4HANA Backend System

- Dynpro Processor (PEP*)
- Business Layer
- Database Layer

Presentation Layer (SAP UI)

- Request
- Response

UIM Configuration Layer
- Roles, Policies (PAP*)
- Sensitive content & context attributes

Original Data

- Transformed Data

Sensitive Content
- Authorization (PDP*)
- Masking Processes

Field Access Trace

External applications (SAP UIL, SAP ETD, analytics, SIEM)

* Legend:
  PAP – policy administration point
  PEP – policy enforcement point
  PDP – policy decision point
The “Logical Attribute” is the central object in configuration: it grouping sensitive context, triggers authorization, and controls consistent application of security actions across UI channels.
Demo
Outlook & Wrap-up
# UI data protection masking

## Product road map overview – Key innovations

<table>
<thead>
<tr>
<th>Recent innovations</th>
<th>2019 – Planned innovations</th>
<th>2020 – Product direction</th>
<th>2021 – Product vision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UI data protection masking for SAP S/4HANA, initial release</strong></td>
<td><strong>UI data protection masking for SAP S/4HANA, feature pack</strong></td>
<td><strong>UI data protection on „SAP S/4HANA Cloud“</strong></td>
<td><strong>UI Data Security bundle on SAP Cloud Platform</strong></td>
</tr>
<tr>
<td>▪ Integrated data element based configurations for data security actions</td>
<td>▪ Integration of Access Trace as a log provider into SAP Enterprise Threat Detection</td>
<td>▪ Technical availability of UI data protection for SAP’s public cloud offering</td>
<td>▪ Technical availability of the UI Data Protection bundle in the SAP Cloud Platform for consumption by SAP SaaS applications</td>
</tr>
<tr>
<td>▪ Data Security actions: masking field values; disabling fields; hiding fields</td>
<td>▪ Data blocking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ “Reveal on Demand”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Access trace (high level technical trace of data processed through UI Masking)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UI data protection masking for SAP S/4HANA, feature pack</strong></td>
<td><strong>UI data protection bundle for SAP S/4HANA, initial release</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Granular and dynamic control which data accesses are masked, logged, notified</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Reveal on Demand with integration framework (e.g. for multi factor authentication, consent management systems)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. This is the current state of planning and may be changed by SAP at any time without notice.
Wrap up

1. Next Generation access controls for securing the intelligent enterprise are dynamic and “attribute based”

2. A generic and flexible framework utilizes “policies” for
   – Defining rules and
   – Utilizing context/attributes existing in SAP systems
Thank you.
Take the Session Survey.

We want to hear from you! Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.
Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:
http://info.asug.com/2019-ac-slides
Q&A

For questions after this session, contact us at uimasking@sap.com
Let’s Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.
Join the ASUG conversation on social media: @ASUG365 #ASUG