

# App Security

## How to Develop Secure Business Apps

SMP Enterprise Grade Mobility – Webinar Series

Martin Grasshoff, SAP Mobile Platform Senior Product Manager  
November, 2013

Brought to you by the SAP Mobile  
Rapid Innovation Group (RIG)

# SAP Mobile Platform: Enterprise Grade Mobility

SCN pages and webinars bring to you technical details on Enterprise Readiness aspects of the SAP Mobile Platform (SMP).

- **Webinars** are done every week Thursday until November. The schedule is published on SCN.  
<http://scn.sap.com/docs/DOC-43425>
- **OnTopicPages** presented links to White Papers, How-To Guides, Blogs and other resources.  
<http://scn.sap.com/docs/DOC-43424>

The screenshot displays the SAP Community Network (SCN) interface. The top navigation bar includes 'Getting Started', 'Newsletters', and 'Store'. A search bar is present with the text 'Search the Community'. Below the navigation bar, there are several menu items: 'Products', 'Services & Support', 'About SCN', 'Downloads', 'Industries', 'Training & Education', 'Partnership', 'Developer Center', 'Lines of Business', 'University Alliances', 'Events & Webinars', and 'Innovation'. The main content area shows a document titled 'SAP Mobile Platform: Enterprise Grade Mobility' created by Jan-G Groeneveld on Jul 2, 2013. The document text discusses mobility solutions as a competitive advantage and the challenges of mobile infrastructure. Below the document, there are social media sharing options for LinkedIn, Twitter, and Facebook. To the right, there is a sidebar with a document titled 'SAP Mobile Platform: Webinars on Enterprise Readiness' created by Jan-G Groeneveld on Jul 2, 2013. This sidebar includes social media sharing options and a list of topics: Enterprise Scale Mobility, Life Cycle Management, Performance, Security, and Supportability. Below the sidebar, there is a section titled 'Webinar Series on SMP Enterprise Grade Mobility' which provides information about the webinar series and a table of webinar topics.

Date	Topic	Links
Jul 11	Introduction to Performance Topics for the SAP Mobile Platform	<ul style="list-style-type: none"><li>Presenter: John Polus</li><li>Recording, Presentation</li></ul>
Aug 8	Load Testing mostly Online Applications (HWC, ODP) with LoadRunner	<ul style="list-style-type: none"><li>Presenter: John Polus</li><li>Recording, Presentation</li></ul>
Aug 15	Load Testing Native Applications with LoadRunner	<ul style="list-style-type: none"><li>Presenter: Dong Pan</li><li>Recording &amp; Presentation: coming soon</li></ul>
Oct 17 New Date	Performance Monitoring & Tuning	<ul style="list-style-type: none"><li>Presenter: Brenda Creaney</li><li>Registration link - soon</li></ul>

# Get More Mobile at SAP TechEd Events

Participate in the InnoJam Challenge to get Hands On Experience with SAP Mobile Solutions



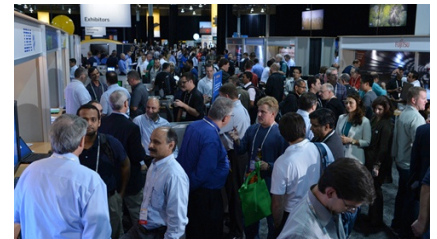
Sign Up for the ASUG Pre-Conference Seminar for Mobile: Deep Dive into SAP Mobile Platform



Attend Education Breakout Sessions to Learn about the latest Mobile Solutions from our Experts



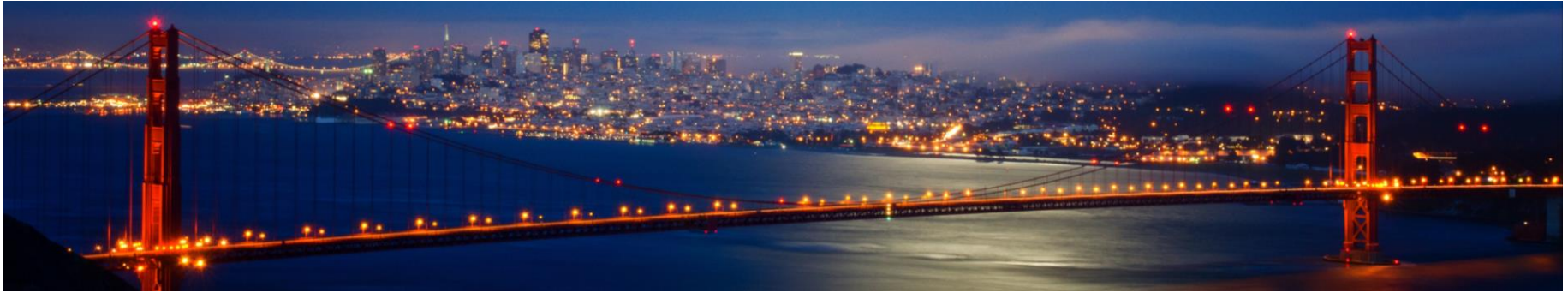
Visit Product Experts at the Mobile Tables on the Technology Showcase Floor



Register Today!

<http://www.sapteched.com>





# App Security

SMP Enterprise Grade Mobility – Webinar Series



# Agenda

---

- 1. Characteristics of App Security**
- 2. Things to know about App Security**
- 3. Q&A**



# Characteristics of App Security

Level 0

# Level 0 - None

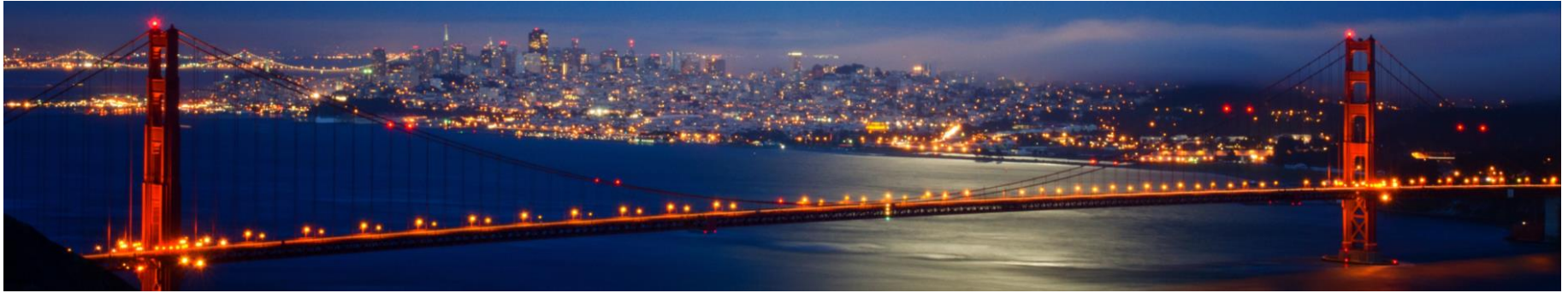
---

**All persons touching the device can access the app and the data**

**Usable for B2C Apps without identification.**

**First step – force locking of device > Afaria**

- **Only persons who can unlock the device can access the app**
- **No coding required, but MDM is needed**



# Characteristics of App Security

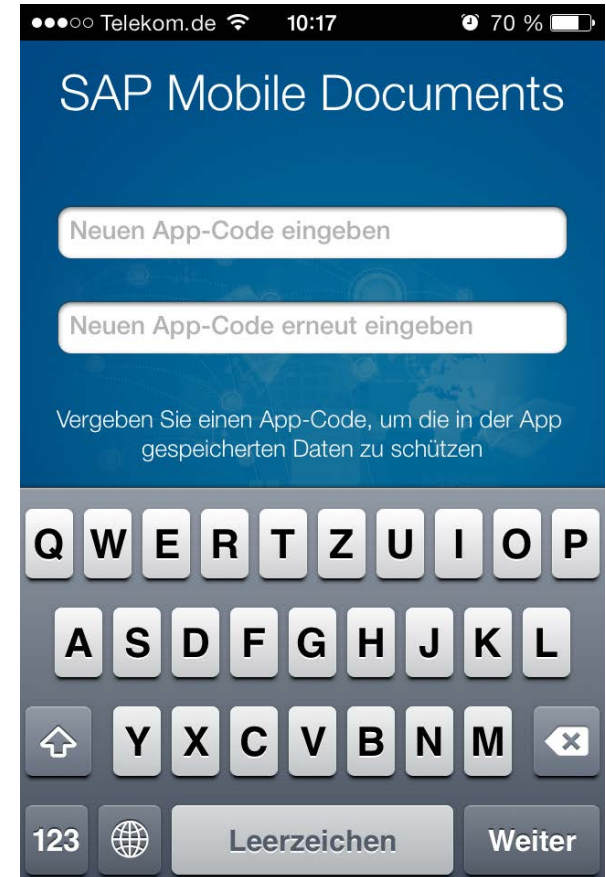
Level 1

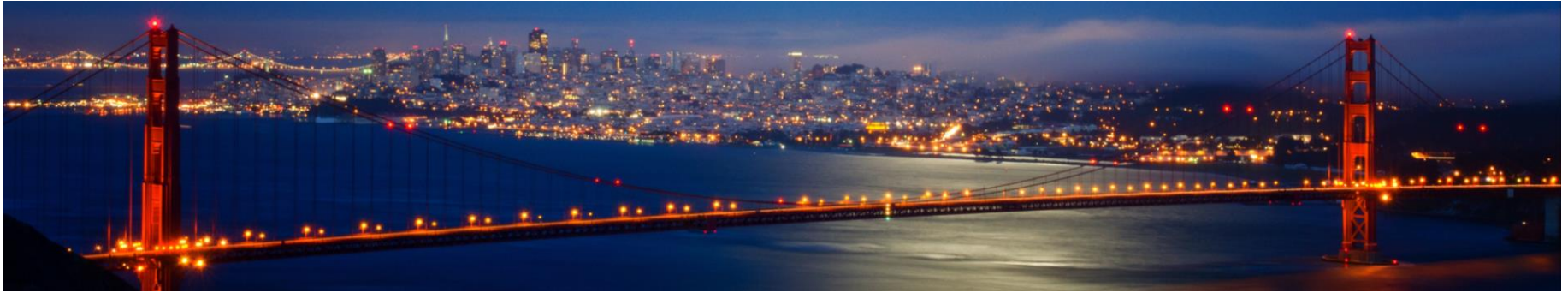


# Level 1 - App Code

## Add an to unlock/open a specific App

- **App specific**
- **Only user knows about it**
- **Can be used as key to unlock encrypted storage**
- **Not available in pure HTML5 Apps**
- **Autolock if App goes to background state**



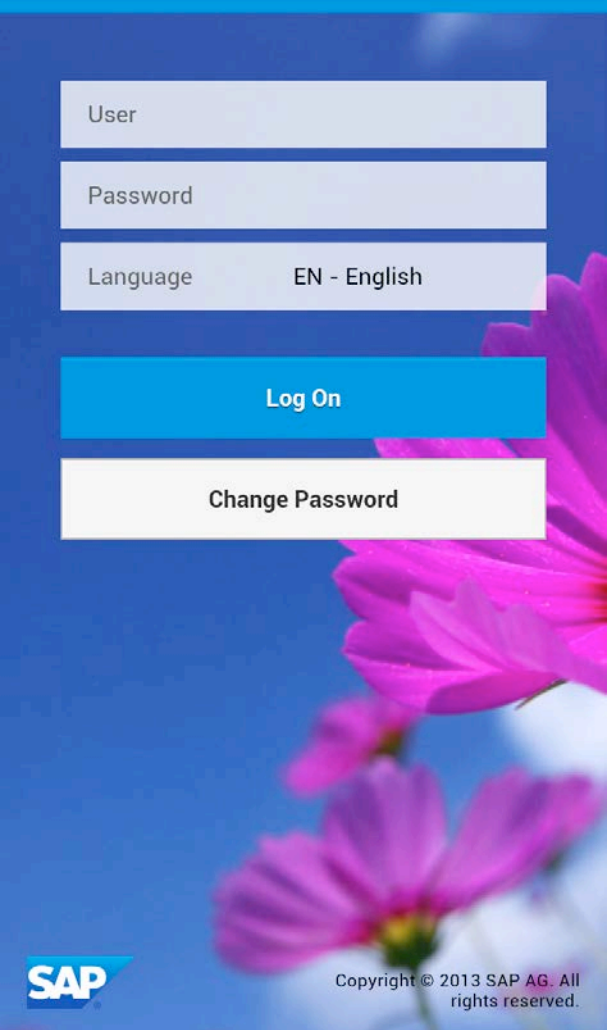


# Characteristics of App Security

Level 2

# Level 2 - Enforce Authentication

- **Backend Credentials or Certificate**
- **For UX store the password in clear text, but encrypted**
- **Let the stored password expire e.g. every week**
- **In B2C allow logon with 3<sup>rd</sup> Party (facebook, google....)**



The image shows a login form on a blue background with pink flowers. The form consists of the following elements:

- A text input field labeled "User".
- A text input field labeled "Password".
- A dropdown menu labeled "Language" with "EN - English" selected.
- A blue button labeled "Log On".
- A white button labeled "Change Password".

In the bottom left corner, there is the SAP logo. In the bottom right corner, there is a copyright notice: "Copyright © 2013 SAP AG. All rights reserved."

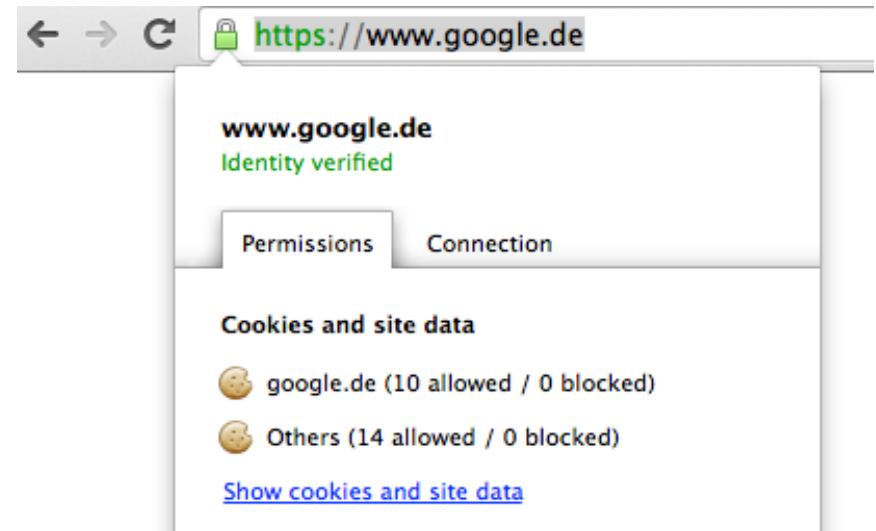


# Characteristics of App Security

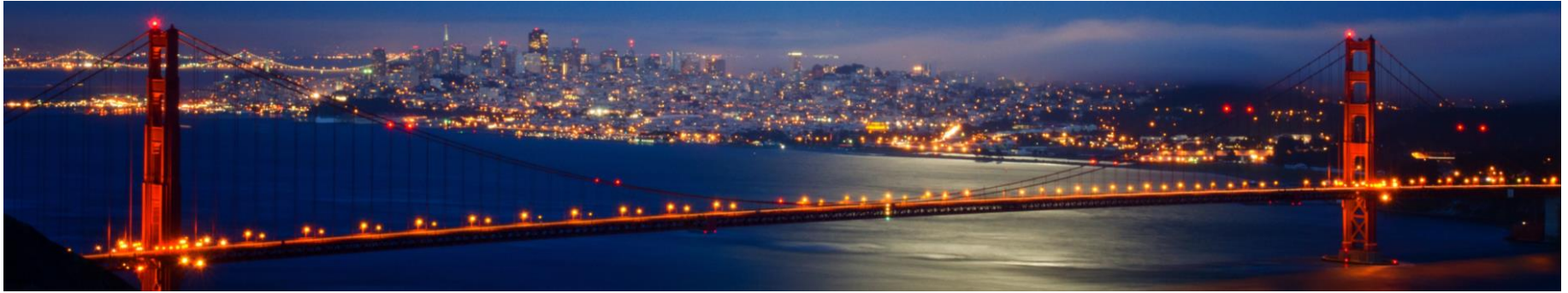
Level 3

# Level 3 – Transport Encryption

- **Use SSL only**
- **Let the user give a chance to check the servers certificate like a browser allows you to do**
- **Use mutual SLL if possible**







# Characteristics of App Security

Level 4

# Level 4 – Encrypt Local Storage

---

- **For UX store the password in clear text, but encrypted**
- **Let the stored password expire e.g. every week**
- **Keystore is secure, but not designed to hold large data volumes**
- **Use UltraLite or sqlcipher to store mass data**



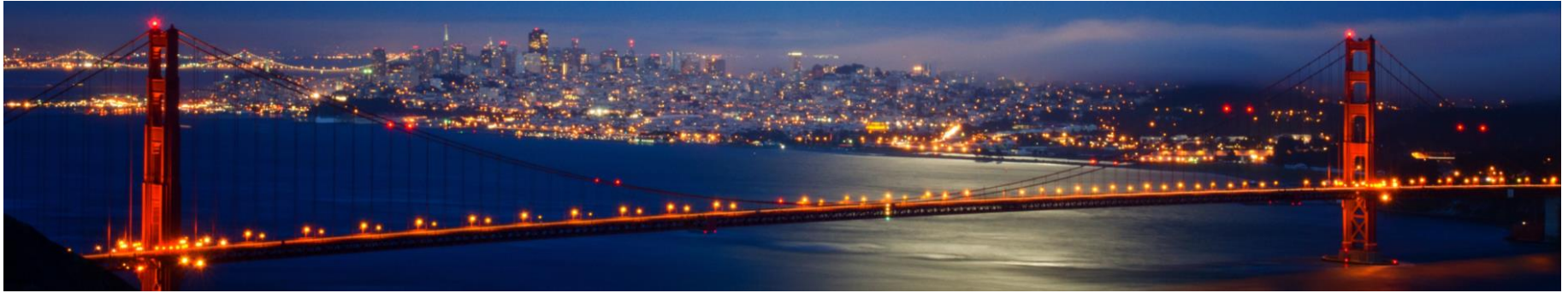
# Characteristics of App Security

Level 5

# Level 5 – No Local Storage

---

- **Data not on the device can not be compromised**
- **Retrieve the data as needed and discard when App enters background state**
- **Don't store password. Let user login every time he uses the App.**



# Characteristics of App Security

Level 6

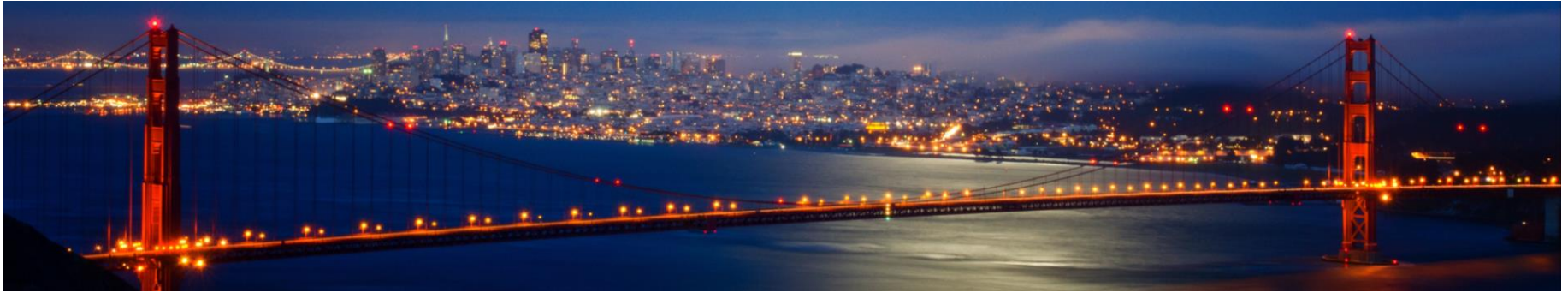




# Level 6 – Prevent Copy & Paste

---

- **Users tend to copy confidential information and send them through unsecured channels, like Email or DropBox and the like**
- **Make sure data can not be copied out of your application**



# Things to know about App Security

Miscellaneous

# Things to know about App Security

---

- WebApps are very vulnerable, so if possible go for native Apps.
- Use Hybrid Apps if native App is not possible.
- Always control user input before sending to backend (SQL Injection, and others)
- Never write your own security component (neither the visible nor the invisible)
- Apply security audits to the whole software development process
- Don't pass security related information to users in error messages. This includes version numbers of Tomcat, stack traces and the like
- Try to categorize data being used to get a feeling for it's sensitivity
- Collect and analyze data on the server side to identify attacks. Automate these audits.
- Know the security implications by your programming language/platform
- Use Certificate Authentication if possible
- Have a plan



# Questions and Answers



# Thank you

Contact information:

Martin Grasshoff,  
SAP Mobile Platform Senior Product Manager  
[martin.grasshoff@sap.com](mailto:martin.grasshoff@sap.com)



# © 2013 SAP AG. 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 AG.

The information contained herein may be changed without prior notice.

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

National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group 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.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.