App Security
How to Develop Secure Business Apps

SMP Enterprise Grade Mobility – Webinar Series

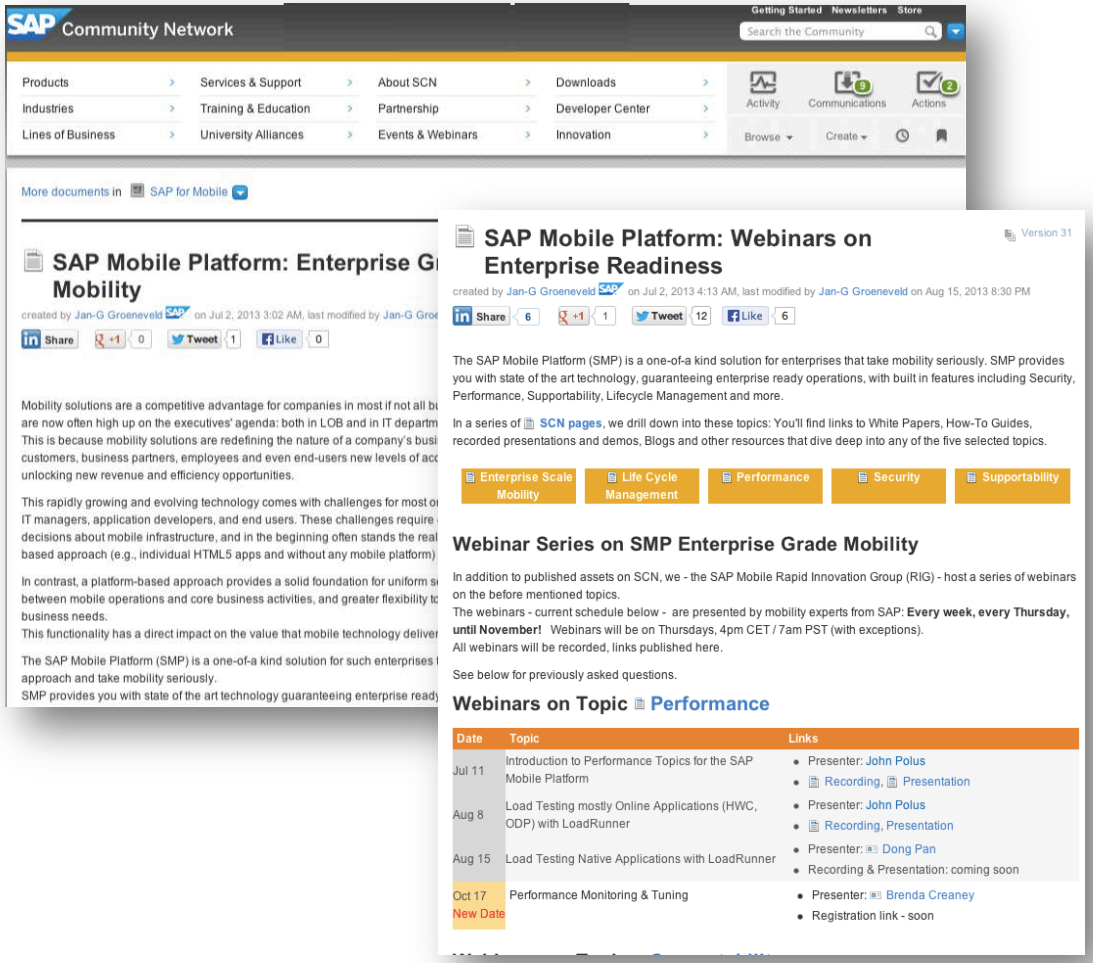
Martin Grasshoff, SAP Mobile Platform Senior Product Manager
November, 2013

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



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.saptech ed.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**

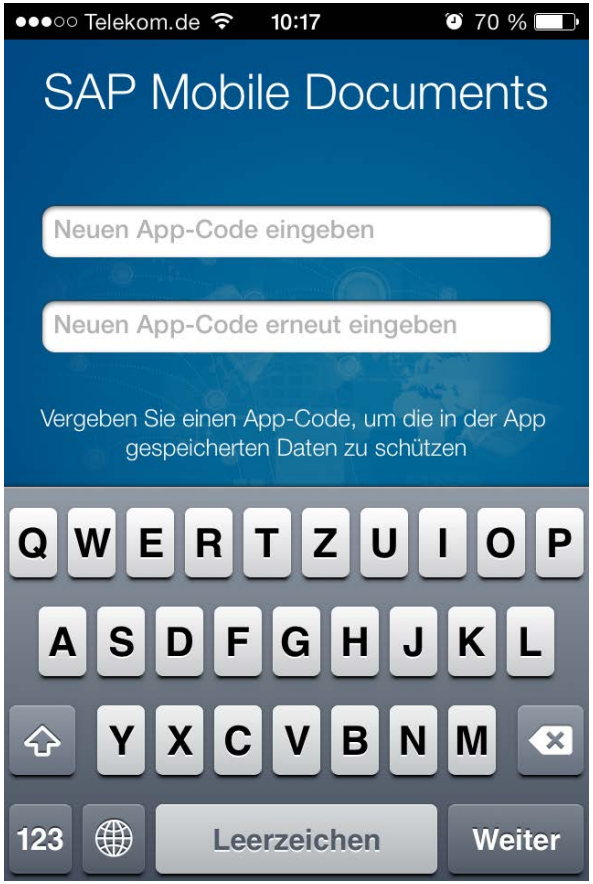
Characteristics of App Security

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**

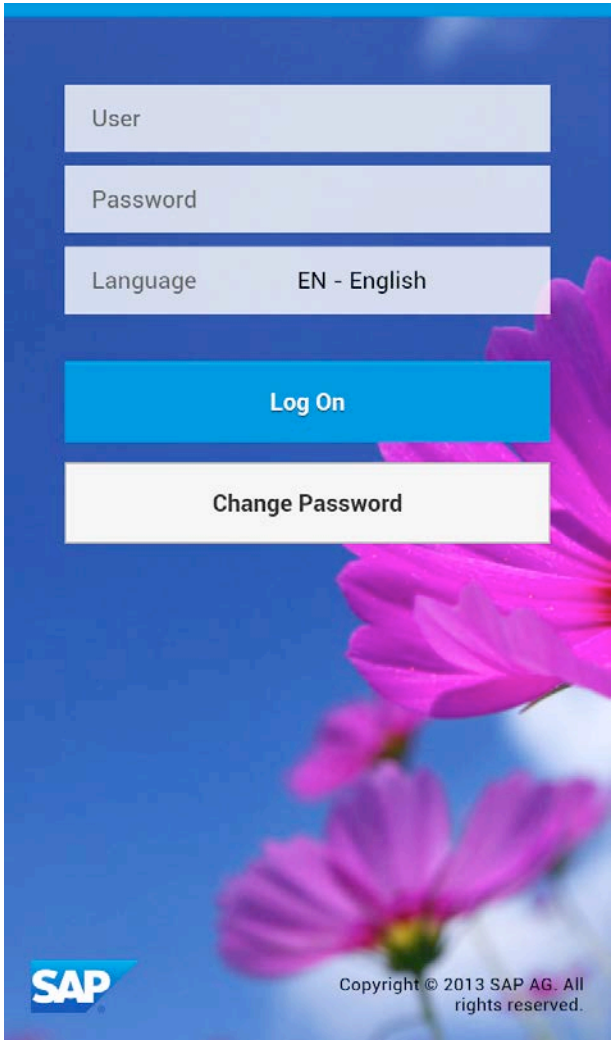


Characteristics of App Security

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 3rd Party (facebook, google….)**



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

© 2013 SAP AG. All rights reserved.